Providing Ideas in Service to Our Nation Since 1955

Center on Terrorism and Counterterrorism
at the FOREIGN POLICY RESEARCH INSTITUTE

Risk and Re-org: Infrastructure Protection in the Commonwealth of Pennsylvania

By Eli S. Gilman

Risk and Re-org:
Infrastructure Protection in the Commonwealth of Pennsylvania

By Eli S. Gilman

December 2011

About FPRI

Founded in 1955 by Ambassador Robert Strausz-Hupé, FPRI is a non-partisan, non-profit organization devoted to bringing the insights of scholarship to bear on the development of policies that advance U.S. national interests. In the tradition of Strausz-Hupé, FPRI embraces history and geography to illuminate foreign policy challenges facing the United States. In 1990, FPRI established the Wachman Center to foster civic and international literacy in the community and in the classroom.

About FPRI's Center on Terrorism and Counterterrorism

Founded in 2002, the Center focuses on terrorists, their strategies and tactics, and their objectives, resources, and capabilities for creating MUD (multilateral unconstrained disruption). FPRI Fellows are also examining the challenges of irregular warfare, strategies for cyber-security, and ways to improve homeland security.

FOREIGN POLICY RESEARCH INSTITUTE
1528 Walnut Street, Suite 610 • Philadelphia, PA 19102-3684
Tel. 215-732-3774 • Fax 215-732-4401
Email fpri@fpri.org • Website: www.fpri.org

Table of Contents

Glossary of Abbreviations

C/ACAMS	Constellation/Automated Critical Asset Management System
CHRIA	Criminal History Record Information Act
CIKR	Critical Infrastructure, Key Resources, and Significant Special Events
DHS	Department of Homeland Security (Federal)
HSGP	Homeland Security Grant Program
HSPD	Homeland Security Presidential Directive
NIPP	National Infrastructure Protection Plan
OHS	Office of Homeland Security (State)
OTS	Off-the-shelf Product
PEMA	Pennsylvania Emergency Management Agency
PSC	Protection Steering Committee
PSP	Pennsylvania State Police
SPP	Site Protection Plan
SSWG	Sector-Specific Working Groups
Title 35	The Pennsylvania Health and Safety Code

1.0 Introduction

On Tuesday, November 22, 2011 Governor Tom Corbett announced that the Pennsylvania Office of Homeland Security (OHS) would be moved from its former location at the Pennsylvania Emergency Management Agency (PEMA) and would instead be co-located with the Pennsylvania State Police (PSP). This move, though not widely reported, is extremely important, as it seeks to address a significant shortfall in a key Homeland Security responsibility: the protection of the Commonwealth's Critical Infrastructure and Key Resources.

Since the events of September 11, 2001, Homeland Security has become one of the most important responsibilities at all levels of government. From the widespread changes brought on by the creation of a new federal department to the increased roles and responsibilities of local first responders, the prevention, protection, response to and recovery from terrorist attacks, natural disasters and other emergencies has become one of the foremost issue areas of the day. New ideas and technologies are constantly emerging to increase institutional collaboration and promote greater program efficiency.

In the Commonwealth of Pennsylvania, however, systemic inefficiencies arose that precluded such progress from being made. In particular, these inefficiencies stifled the ability of the state to perform virtually any of its Critical Infrastructure Protection duties, which are intended to facilitate the resiliency of the Commonwealth through the identification of assets, the analysis of risk, and the development of strategies to mitigate that risk. While some attempts were made to address these issues in the decade since September 11, 2001, the results mostly exacerbated the existing issues rather than instilling any long-term solutions.

Now, though, with OHS being co-located with the State Police, the opportunity exists for just such a solution to come about. First and foremost, this move will enable better coordination between the intelligence gathering operations at the State Police and the intelligence dissemination functions of the Office of Homeland Security. More important still, this move will position the Office of Homeland Security to offer greater protection of Pennsylvania's critical infrastructure and key resources.

2.0 Situation

The protection of critical infrastructure, key resources and significant special events (collectively referred to as *CIKR*) is essential to the Nation's security, public health and

safety, economic vitality and way of life.[1] Attacks on CIKR could significantly disrupt the functioning of both the government and the private sector. Terrorist attacks, major disasters and other emergencies—referred to now as *all-hazards incidents*—may result in catastrophic losses in terms of human casualties, short and long-term economic inconsistencies and profound psychological damage to public morale and confidence. Moreover, because CIKR exist within an interdependent network of critical systems and assets, such attacks would likely produce cascading effects well beyond their targeted sectors or physical locations.

The Commonwealth of Pennsylvania is the nation's sixth largest state with a population of over 12 million people. It boasts significant rail lines and highways, two major international airports, military installations, key ports, critical industrial sites, sizable agricultural support and processing facilities, and five nuclear power plants. Two of the Nation's most cherished historical icons—the Liberty Bell and Independence Hall—reside in Pennsylvania, along with dozens of other historical and cultural sites. More than 20 major sports and entertainment venues bring tens of thousands of people together for special events year-round. Pennsylvania is positioned between the two cities directly attacked on September 11, 2001 and near an international border, making the Commonwealth citizenry keenly aware of the need to protect themselves against the threat of terrorism and the effects of a major disaster.

All levels of government must collaborate to secure these vital assets against all-hazards incidents. They must tailor strategies aimed at protecting CIKR from, or making them more resilient to, all-hazards threats. Subsequently, the development of integrated protection plans requires that all levels of government engage the private sector in collaborative dialogue to create sustainable and security-focused relationships. Because roughly 85 percent of all CIKR resides within the private sector, the success of any critical infrastructure protection activity depends on the ability of these government agencies to form trusting relationships with private industry.

Relationship building must also extend to the Federal government, since it sets the overarching guiding policies for Preparedness-related initiatives. State-level infrastructure protection activities should be linked directly with the National Infrastructure Protection Plan (NIPP) and other Federal programs in order to achieve full effectiveness. Through Congressional legislation, Presidential Directives and Department of Homeland Security (DHS) guidelines, Commonwealth activities must continuously evolve to address and meet

[1] According to the Critical Infrastructures Protection Act of 2001, the term *critical infrastructure* refers to those "…systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The term *key resources* means publicly or privately controlled resources essential to the minimal operations of the economy and government.

Federal standards while still complying with state-level governance structures. In particular, because DHS guidelines for programs such as the Homeland Security Grant Program (HSGP) change annually, investment justifications tied to CIKR protection should reflect those changes while continuing to support the strategies created by the state.

At the state-level, successful implementation of infrastructure protection is dependent upon the unique socio-political characteristics and governance structures that define each state's institutional culture. In the Commonwealth, Homeland Security functions are spread across multiple agencies with the authority for each core mission area (Prevention, Protection, Response and Recovery) assigned to a different entity. Prevention activities are conducted by the Pennsylvania State Police; protection activities by the Office of Homeland Security; and response and recovery activities by the Pennsylvania Emergency Management Agency, which also acts as the State Administrative Agency for all Homeland Security grants coming into the Commonwealth. Because of the wide-ranging nature of Homeland Security activities, a number of other state agencies have jurisdiction over specific policy areas and therefore play a significant role in all four of the mission areas. For the Commonwealth's infrastructure protection mission in particular, the role of these agencies is critical as they represent the state's subject-matter-experts for their respective sectors.

Beyond state level, coordination with county and local governments is also essential. Not only are they more familiar with their respective geographical area, but Congressional directives mandate that 80 percent of all HSGP funds be distributed to local municipalities to increase the capabilities of their respective first responder community. To facilitate this distribution in such a large state, the Commonwealth set up nine Regional Task Forces comprised of locally elected leadership, appointed officials and chief representatives for first responders of member counties. These task forces also consist of representatives of county organizations, including: emergency management agencies, law enforcement, fire/rescue, emergency medical service and state certified hazardous material response teams. Other county officials such as sheriffs, district attorneys and coroners may also participate, though each task force sets its own membership guidelines. The task forces are responsible for developing spending plans for the local allocations of HSGP funds, as well as for coordinating the training and exercises that take place within the region. However, coordination between the state and task forces proved to be seriously complicated because of a lack of legal tasking authority on the part of both entities with regard to their respective subordinate polities. In addition, conflicts arising between representatives of member counties also impeded continuity. Regarding infrastructure protection, this severely hindered the ability of OHS to partner with these task forces and to collect information about assets within their respective regions.

More specifically, OHS attempted to leverage the unique knowledge of the task forces in three ways. First, they were used to identify assets. When OHS began to collect information from the task forces, it asked the task forces to provide a list of CIKR for the counties within their respective regions. This information was then combined with a list of state agency-identified CIKR to form the first comprehensive list of CIKR in Pennsylvania. However, a low level of feedback from the counties severely hindered OHS's ability to gather all relevant data; possibly due in part to the lack of authority of OHS to task the counties and regions for support. Another way in which OHS sought to leverage the task forces was in the assessment of CIKR facilities. OHS, along with local representatives of DHS, are responsible for coordinating DHS-sponsored Site Assistance Visits and Buffer Zone Protection Plan Assessments. These vulnerability assessments are intended to provide county emergency management officials and local first responders with information about a particular site that would allow them to better plan for an all-hazards event, while at the same time providing CIKR owners and operators with specific potential improvements (or *options for consideration*) to their security posture. In large part, the task forces consistently took part in these assessments, although their role in many cases was to introduce the services they offer to each site they visited, rather than to actually gather facility-specific information.

Finally, OHS attempted to leverage the task forces in the protection of their respective CIKR through the allocation of funds to support and enhance the capabilities needed to respond to and recover from all-hazards events affecting specific facilities. This occurred in two ways, both of which were tied directly to Pennsylvania's annual HSGP allocation. First, the task forces were asked to provide specific information about their respective CIKR that would have increased the chances of those facilities being included in that year's list of federal assets. As 15 percent of DHS's allocation formula revolves around the amount of CIKR in each state, this, in turn, would have increased the amount of money allocated to Pennsylvania in the subsequent HSGP allocation. Second, once the task forces were given their respective allotments, they were asked to use 15 percent of that money to protect identified CIKR. However, since this was a relatively new request by the state, and more specific guidelines were never fully developed, most of these funds have only been used to support and enhance County Emergency Operations Centers.

It is also important to note the effects that specific events have had on the organizational and governance structures of Homeland Security, and more specifically Infrastructure Protection activities, in the Commonwealth. Prior to the events of September 11, 2001, the primary focus of domestic preparedness was emergency management. As such, PEMA had the lead role in coordinating the response activities to events deemed too large for the counties to handle. While there was a great deal of emergency planning involved for regular events, such as flooding in the Northeast part of the state, little thought was given

to the potential effects that terrorist incidents could have on the ability of the government to continue to provide essential services to its citizens. Inter-agency and regional collaboration at that time was virtually nonexistent, making it extremely difficult to mount a sufficient response to events that crossed jurisdictional or physical boundaries.

After September 11, 2001, however, institutional dynamics changed drastically. Presidential Directives and Congressional legislation enabled the creation of a new federal department responsible for all four of the core Homeland Security mission areas, thus incorporating the prevention and protection roles into the range of its activities. State and local governments were asked to play a larger part in this important mission through enhanced collaboration with the federal government, the fusion of intelligence information, and a new focus on the identification and protection of CIKR.[2] At the state level, this was accomplished through Executive Orders that established a new Homeland Security organizational structure consisting of OHS (now responsible for coordinating all Commonwealth Homeland Security activities); a Homeland Security Executive Cabinet of state officials in the various agencies, whose jurisdictions were commensurate with such activities; and a Homeland Security Advisory Council of state officials and representatives of various industries. Ultimately, the goal of these new institutions was to synthesize different perspectives regarding potential Homeland Security issues and provide recommendations to the Governor about how those issues might be mitigated.[3]

Lessons gained from subsequent events, especially the responses to Hurricanes Rita and Katrina, have also altered the Homeland Security Organizational Structure nationwide. However, no event has shaped the direction of such activities within the Commonwealth more than the state's inadequate response to the ice and snow storm that occurred February 13-14, 2007. A lack of inter-agency communication and pre-determined leadership plagued the response to the storm, leaving hundreds of motorists stranded on Pennsylvania's highways for hours as state officials tried to clear the more than 50-mile traffic jam. The resulting study conducted to assess the current Emergency Management Organizational Structure proposed many changes designed to increase collaboration, to encourage pre-defined disaster response leadership positions, and to institute a new

[2] The following legislation provides the specific guidance and key authorities for this mission: The USA PATRIOT Act of 2001, the Foreign Intelligence Surveillance Act of 1978, the USA Act of 2001, the Financial Anti-Terrorism Act of 2001, the Homeland Security Act of 2002, and the Implementing Recommendations of the 9/11 Commission Act of 2007. Additionally, Homeland Security Presidential Directives (HSPD) 3, 5, 7 and 8 are of particular importance, here, as they establish the Homeland Security Advisory System; the National Incident Management System and the National Response Plan; the National Infrastructure Protection Plan; and the National Preparedness Goal, National Planning Scenarios, Universal Task List and Target Capability List respectively.

[3] PA Executive Order 2002-11 was the first to establish this organizational structure and set state-wide priorities for Homeland Security activities in the Commonwealth. Subsequent Executive Orders 2006-05 and 2007-10 have altered this mission and organizational structure to reflect newer federal guidance, organizational growth and shortcomings that have been identified through the insufficient response to certain events.

Homeland Security Organizational Structure that brought the responsibilities of Infrastructure Protection underneath the purview of the PEMA Director.[4]

Chief among the recommendations was the creation of a new Department of Emergency Management and Homeland Security that would place OHS and its Infrastructure Protection duties underneath PEMA. Though this recommendation was never fully implemented due to the legislative constraints surrounding a revision of the Commonwealth's Health and Safety Code (Title 35), the state did begin to reorganize the Homeland Security organizational structure to align itself with this revision's eventual passage. First, Governor Edward Rendell issued Executive Order 2007-10, which dissolved all pre-existing executive cabinets and advisory councils and altered the governance structure to give PEMA overall authority in all four of the Homeland Security mission areas, making OHS report directly to the PEMA Director. It also established the Governor's Preparedness Interagency Executive Management Committee to coordinate the Commonwealth's Preparedness plans, procedures, policies, resources, and capabilities necessary to fulfill its responsibilities in all aspects of Homeland Security planning.

Subsequently, PEMA began to develop a new organizational structure with the help of the Governor's Office, the Office of Administration, and the Office of General Counsel. This new structure went into effect on November 1, 2009 in anticipation of an eventual revision of Title 35 and the creation of the new Department. However, almost two years and an administration later, neither of these items occurred. Likewise, Infrastructure Protection played nearly no role underneath this new structure, as OHS no longer existed within it, and was instead replaced by just two positions in what was called the Division of All-Hazards Planning. While it had been said that OHS's core Infrastructure Protection planning functions would still exist within this Division, such a structure severely limited its ability to maintain a constant focus on the identification, assessment and protection of the Commonwealth's CIKR.

Nevertheless, with the announcement by Governor Corbett that OHS would now be moving to PSP, the opportunity exists for Infrastructure Protection to once again be made a priority. In fact, co-locating the office with PSP makes perfect sense for the simple reason that it will allow for the direct sharing of intelligence information between those who are charged with gathering it and those who are charged with disseminating it to the private sector. Moreover, breaking OHS out of the response and recovery driven policies of PEMA

[4] This report was conducted by the James Lee Witt Associates, who was contracted by the Governor. A full synopsis of their recommendations can be found in their final report at http://www.portal.state.pa.us by searching for the document entitled, "PA_Report_Final.pdf."

will finally give the office the support it needs to develop and implement the policies and programs necessary to carry out its duties under the Infrastructure Protection mission.

Though only time will tell whether or not the organizational shift will accomplish these goals, it is apparent that the current administration recognizes that OHS would never have been able to fulfill its objectives if left as a small division within PEMA. Nonetheless, it is important to complete a thorough analysis of the Commonwealth's Infrastructure Protection mission in order to review the mistakes that were made in the past, and to ensure that they are not repeated under the new structure. The following sections, therefore, will review the objectives, mission, and means by which these responsibilities both have been and should be carried out in Pennsylvania.

3.0 Objectives

Any successful infrastructure protection program requires, first and foremost, a reduction of the overall risk to its respective set of CIKR. And because, pursuant to HSGP guidelines, this must be measured by the enhancement of local first responder capabilities, state-centered risk-mitigation strategies must be able to deter threats, reduce vulnerabilities and mitigate potential consequences by the effective dispersal of all allowable HSGP funding and other state resources. Thus, a measured reduction in risk can only occur by ensuring that all available funding is allocated in accordance with some measure of calculated risk that identifies and prioritizes gaps in target capabilities, and which can be used universally across all sectors. In addition, successful implementation of such a program requires the sharing of complete, accurate, and reliable critical infrastructure information among other governmental and private sector partners.[5] This fosters situational awareness and enhances emergency response planning by both the private sector and first responders. Achieving this will also give each entity its own capability to assess risk and to execute the necessary risk mitigation plans.

In order to accomplish these goals in the Commonwealth, OHS instituted a structure where risk mitigation is derived through a continuous cycle of the following six objectives: setting

[5] According to the Critical Infrastructure Information Act of 2002, the term *critical infrastructure information* means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. This refers to (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety; (B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or (C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

security goals, identifying assets, assessing their respective risk, prioritizing assets and funding priorities, developing protection strategies, and auditing and reevaluating the success of the process.

Objective #1: Set Security Goals

Overarching security goals must be set before anything else can be accomplished. These goals must be both realistic and attainable, and provide the necessary guidance for the succeeding objectives. Generally, they must also encompass three considerations for steady-state operations: specific, attainable outcomes; the probable conditions—or scenarios—under which protection capabilities might be needed; and the end points—or target capabilities—for which first responders and CIKR owners and operators should aim.

Objective #2: Identify CIKR

The second objective requires the identification of all assets, systems and networks deemed vital to the Nation and to the Commonwealth. However, successful implementation of this objective also requires developing proper methods of classification based upon industrial sector and relative level of criticality. Using a consistent, structured terminology allows for the designation of CIKR as belonging to a particular group, which can then be broken down into various sub-group levels to better understand the asset and describe its functions.[6] Once this has been designated, sector-specific criteria must be developed to assess the criticality of each site using a standard, applicable method. Additionally, because CIKR and their elements can be described in different ways, such classification needs to be consistent across all levels of government. Failure to do so could result in conflicting terminologies that may impede communication and obstruct the decision-making process during an emergency.

Objective #3: Assess Risks

Once the CIKR have been identified, it is necessary to determine, on a universally consistent basis, the overall risk that can be attributed to each site, to provide an accurate comparison across sector and jurisdictional boundaries. To accomplish this, a formula must be developed that accurately depicts the level of risk as a function of a site's vulnerability to disruption from an all-hazards incident, the perceived threat against it, and the likely consequences of such a disruption. And because such a formula is inherently based upon

[6] For the purposes of this objective, the DHS Infrastructure Taxonomy is used to classify CIKR based on Sector, Sub-sector, Segment, Sub-Segment and Asset Type. The 18 sectors are comprised of Agriculture & Food, Banking & Finance, Chemical Facilities, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Government Facilities, Information Technology, National Monuments & Icons, Nuclear Facilities, Postal & Shipping, Public Health & Healthcare, Transportation, and Water.

subjective analyses, it must also be able to convert this information into a numerically-derived, justifiable estimation of risk. To do so, each of the three variables in this formula (Vulnerability, Threat and Consequence) must have their own mechanism for eliciting a numerical value from available information. These values can then be synthesized into an overall risk score that can be compared to the scores of other CIKR to determine which sites are most at risk. However, this does not yet provide a complete picture, because the existing capabilities to mitigate the perceived risk have not been identified. Once this is achieved, a risk profile can be generated that shows where the greatest gaps exist in the capabilities to prevent, protect, respond to, and recover from an all-hazards incident at each of the most at-risk CIKR. Such a tool will be most beneficial to coordinate protective measures, prioritize investments, and ensure that funding is allocated in an effective and efficient manner.

Objective #4: Prioritize

Such risk profiles make it possible to prioritize funding first responder activities, equipment, planning efforts, and exercises. This prioritization will serve to link such initiatives to the annual HSGP allocation, as 80 percent of the funding from this grant is designated for such efforts. However, it is important to note that prioritization is a dynamic process. New threat factors affecting each sector of CIKR surface daily and other, newly collected information regarding site-specific vulnerabilities or regional capabilities can dramatically affect the urgency of capability enhancements. This prioritization methodology allows planners to quickly account for changes to the inputted information without making wholesale adjustments.

Objective #5: Develop Protection Strategies

The complete protection of CIKR will be the most difficult objective to attain. With over 85 percent of all CIKR residing in the private sector, enhancing the response capabilities of first responders through the HSGP will only accomplish so much. Paramount then is gaining the participation and support of the CIKR owner/operators because the best efforts to identify, prioritize, and fund the needs of first responders are meaningless unless owner/operators feel the same urgency to invest in their own security. Legal restrictions prohibit the state from providing physical security enhancements to private sites, so protection strategies must be based upon the coordination of training programs, detection efforts, and other protection measures between all levels of government and the private sector. The Commonwealth can recommend resiliency strategies by providing opportunities to share lessons-learned and best practices on an industry-wide basis, while at the same time enhancing the collaboration between CIKR and their respective first responder community. On the other hand, it should also be possible to provide site-specific

enhancement strategies through the effective collection of site-specific vulnerability information. Options for consideration—though in no way binding—can enable CIKR owner/operators to gain a better understanding of their facilities' shortcomings. CIKR owner/operators can then make their own cost/benefit analyses to determine what security enhancements should be made without increasing their liability.

Objective #6: Measure Effectiveness

Like the prioritization process, measuring the effectiveness of infrastructure protection activities is also a continuous effort. A mechanism is needed to perform periodic capability assessments to identify improvements among the necessary target capabilities. Not only is this due-diligence, but the results obtained through this process will determine if—and how well—pre-existing gaps in the target capabilities have been filled, which in-turn will drive future funding strategies. Evaluation of the relative success of this entire program may necessitate revisions to better implement the overarching goals of infrastructure protection.

4.0 Mission

Because of Pennsylvania's unique governance structure, successful implementation of these infrastructure protection objectives requires the collaboration of many different agencies that have subject-matter expertise in their respective areas, as well as the sustainability of close relationships between all levels of government and the private sector. In order to facilitate this, OHS originally set up a Protection Steering Committee (PSC) responsible for the development of overarching initiatives and oversight of protection-related strategies for CIKR. The PSC comprised representatives from the Office of Homeland Security, the U.S .Department of Homeland Security, the Pennsylvania State Police, the Pennsylvania Emergency Management Agency, the Department of Military and Veterans Affairs, the Office of Administration, and the Office of PennPorts. In addition, the PSC was supported by seven Sector-Specific Working Groups (SSWG) whose chairs also sat on the steering committee. The SSWG encompassed each of the 18 sectors identified in the NIPP, and were composed of the various state agencies that shared jurisdiction over their respective sectors. The groups were responsible for advising OHS and its local/regional and private sector partners on issues pertaining to their respective subject areas.[7]

[7] The seven SSWG and their respective lead agencies are as follows: the Agricultural Working Group –Department of Agriculture; the Commercial Facilities Working Group – Department of Labor and Industry; Energy and Environmental Working Group – the Department of Environmental Protection; the Government Facilities Working Group – Department of General Services; the Information Technology and Telecommunications Working Group – Office of Administration-Office of Information Technology; the Public Health Working Group – Department of Health; and the Transportation Security Working Group – Department of Transportation.

At first, OHS had also set up an Advisory Council made up of private sector and regional task force representatives to include their viewpoints on potential Homeland Security issues. However, pursuant to Executive Order 2007-10, this Advisory Council was abolished, and OHS had to rely more heavily on private sector participation in each of the different SSWG to gain their perspective. But because the SSWG were made-up of the state agencies that regulate private industry in their respective areas, this remained a difficult task indeed.

Regardless, the PSC and SSWG were instrumental in the development of overarching security goals that determined the direction of the other infrastructure protection objectives. Regular meetings allowed for updates and revisions to these goals as new issues arose, the synthesis of which enabled OHS to better develop the tools necessary to carry out its intended mission. Additionally, such meetings facilitated the development of Pennsylvania-specific planning for worst-case scenarios to protect the Commonwealth and its CIKR. These scenarios, while taken from the original fifteen outlined in HSPD 8, were altered to reflect the Commonwealth's unique geological/meteorological and industrial characteristics, as well as the addition of certain scenarios, such as Armed Intruders, that had previously been neglected.[8] Moreover, HSPD 8 also provided the Commonwealth with the 37 Target Capabilities necessary for the effective prevention, protection, response to and recovery from all-hazards incidents.[9]

The identification of CIKR, however, continued to be a much more laborious—and ultimately frustrating—process. While the classification methodology provided by DHS in the Infrastructure Taxonomy was useful for identifying assets, the lack of a consistent definition of what constitutes criticality has deterred concrete prioritization of the Commonwealth's CIKR. In fact, the constantly changing definitions used by the federal government to determine nationally critical assets further complicated this process. To mitigate this, OHS had asked the SSWG to develop sector-specific criteria, but varying levels of agency participation within the SSWG slowed this. The Commonwealth, therefore, used a more subjective method to identify its CIKR, relying on the institutional knowledge of each agency and a "boots on the ground" approach. Certainly, this method produced a comprehensive list of the Commonwealth's CIKR, but without a clear definition of what constitutes criticality, this list will always be sub-optimal.

[8] There are 10 Pennsylvania-Specific Planning Scenarios. These include: Nuclear Detonation, Biological-Agricultural, Biological-Food, Chemical-Toxic Industrial, Chemical-Weaponized Agents, Natural Disaster-Hurricane, Natural Disaster-Winter Storm, Improvised Explosive Device, Cyber Attack, and Armed Intruder Assault

[9] The full list and descriptions of each capability can be found in the National Preparedness Guidelines, which can be accessed at http://www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf.

Conversely, the assessment of risk was a much more successful endeavor. With the help of the PSC and SSWG, OHS was able to develop basic measures for vulnerability, threat and consequence. Using a mathematical algorithm weighted by current threats, OHS was able to synthesize these measures into a relative value of risk for each identified asset. To analyze vulnerability, OHS sought to steer away from conventional analyses that focused primarily on physical and systems security by also including other vulnerabilities like administrative-personnel issues and financial viability. Threat was accounted for by analyzing the likelihood that a particular asset will be affected by each of the ten Pennsylvania-specific planning scenarios, and through an analysis of current intelligence that allowed for each sector to be ranked according to the adversarial intent to cause harm, the enemy capability to carry out the intended attack, and the historical trend of similar acts throughout the world. In the OHS algorithm, the value obtained by this measure was the most heavily weighted because if there was no threat, vulnerability and consequence became far less significant. The final variable, consequence, was defined as a function of public health impacts, economic impacts, government mission impacts and psychological impacts. These impacts were measured by injuries and fatalities, real dollars, the length of time such services would be disrupted, and the likelihood of an incident causing widespread digression from normal behavior. Not only would the values obtained by this measure have been used in the risk algorithm, but overlaying these scores with each of the planning scenarios would have provided an analyst with an extremely beneficial indicator for determining which scenarios had the worst potential consequences across all sectors.

By completing these assessments Commonwealth-wide, OHS would have been able to determine the set of most at-risk CIKR, and then to compare that list to identified shortcomings in the capabilities of first responders at the local, county and regional levels to determine funding priorities. And, since funding is a finite resource that is tied to each year's HSGP allocation, OHS would have been able to prioritize all potential investments so as to mitigate those identified shortcomings in the most effective, efficient, and justifiable manner. Unfortunately, the Commonwealth was not able to accomplish this due to insufficient tools and resources at the state level. For example, a comprehensive CIKR Database program that would have been able to perform this function on an ever-changing basis was necessary for its completion, but because of depleting state budgets and obstructive bureaucratic mechanisms, such a database was never developed. Instead, the Commonwealth relied upon a measure using population and economic data, as well as the amount and type of CIKR within each region to determine the specific quantities of HSGP funds allocated to each region. While this measure did prioritize funding initiatives based—at least in part—on identified CIKR, it did not allow for any prioritization based on the associated risk attributed to them. The development of such a risk-based database program is, therefore, essential to the successful completion of this objective; without it, the Commonwealth's prioritization methodology will remain insufficient.

Until the preceding objectives have been met, the Commonwealth cannot begin to develop specific protection strategies aimed at reducing the risk to individual CIKR, as well as the risk attributable to each sector/industry and, ultimately, Commonwealth-wide. In order to mitigate this, OHS began development on what it called, the Site Protection Plan (SPP) Program. This program was designed to elicit site-specific information through the use of the comprehensive vulnerability assessment necessitated by the third objective. Comparison of these protection plans would have enabled the identification of Best Practices and Common Vulnerabilities within individual sectors, allowing for the development of strategies aimed at reducing the respective risk to each one. In turn, these strategies would then have been blended together to form a Commonwealth-wide risk mitigation strategy aimed at identifying the overarching factors that contributed to the Commonwealth's risk, while providing substantial mechanisms for its reduction. However, pursuant to the restructuring of the Infrastructure Protection mission under PEMA in 2009, work on the development of the SPP program was curtailed, leaving this objective virtually unattainable.

Unless the gaps prohibiting the completion of the preceding objectives are addressed, there is no way to effectively measure a reduction in risk to the Commonwealth's CIKR, or to assess the overall viability of Pennsylvania's Infrastructure Protection Program. Instead, PEMA relied on systematic audits of the Regional Task Forces' expenditures to see if they simply fell in line with the state's overarching strategy, and with the individual state spending plans developed prior to the disbursement of HSGP funds. Nevertheless, PEMA did conduct a state-wide capability assessment in 2009 to develop the baseline capabilities present within each region, and to be better positioned to measure future progress. However, data from this analysis may prove to be relatively unusable because sufficient information was not collected with regard to county or local level capabilities, and because evaluators were asked to reduce their initial estimates to show greater improvement in subsequent evaluations. The Commonwealth is therefore currently ill-equipped to measure its ability to enhance target capabilities. New methods and tools should be developed to better capture this information.

5.0 Means

Specific tools have been—and more still need to be—developed for the Commonwealth to effectively reduce the risk associated with its CIKR. In some cases, this simply requires the development of strong, lasting relationships between varying levels of government and the private sector. In others, it requires creating justifiable measures by which to collect

information and the tools needed to analyze what has been collected. Depending on available resources, these tools may be "off-the-shelf" (OTS) products purchased for use by the Commonwealth, created exclusively for the Commonwealth by a hired contractor or developed in-house by OHS or another State agency. Each of these three options, though, has its own trade-offs that state officials must weigh before deciding upon a course of action. The use of OTS products, for example, may be cost-effective, but they neglect any of the unique characteristics of infrastructure protection created under the Commonwealth's program, (such as the ten Pennsylvania-Specific Planning Scenarios) or its measure of vulnerability. Customizing such products by an outside contractor may be an available option, but that would almost certainly require more money, reducing its cost-effectiveness. Creating the product in-house may be inherently cheaper but officials need to be mindful of the service costs of using employees on projects other than their assigned jobs. Ultimately, the only wrong decision would be to leave the Commonwealth without any tools to determine effective and efficient investments.

In addition to the creation of certain tools like the Pennsylvania-specific Planning Scenarios and the identification of target capabilities, successful completion of the first infrastructure protection objective requires consistent support from the other agencies that were represented in the PSC and SSWG. Because of the organizational structure under which the infrastructure protection mission must operate in the Commonwealth, the continued support of these agencies is essential if the Commonwealth wants to include the state's various subject matter experts in the development of its security goals. However, the fact remains that infrastructure protection is not their primary responsibility, nor is it usually their second or third, so maintaining their support and cooperation is a difficult task when faced with conflicting duties. In practice, this has proven to be the case, as various levels of cooperation among the other state agencies led to the neglect of various projects and poor attendance at regular meetings. In light of these realities, the Commonwealth should better define the responsibilities of these agencies under the Homeland Security Organizational Structure. Whether by executive order or as part of a Title 35 Revision, responsibility under the Infrastructure Protection mission needs to be codified in a manner consistent with its objectives.

Specific tools also need to be generated to best complete the identification of CIKR. While OHS has been able to capture enough information using available methods relative to the progress of its infrastructure protection program, the ensuing list of assets has been sub-optimal because no consideration has been given to specific quantitative metrics that can better inform analysts of their relative level of criticality. In essence, for each asset classification type there needs to be at least one threshold level at which an asset becomes critical to the Commonwealth. For example, 20,000 seats could be an acceptable threshold level for an arena; water treatment plants that service at least 100,000 people could be

acceptable for that type of facility; and a height of 850 feet could be an acceptable threshold for commercial office buildings. Non-numerical thresholds can also be used to ascertain the criticality of chemical sites storing hazardous materials, pharmaceutical companies producing important vaccines, as well as smaller critical manufacturers of products deemed vital to sustaining other assets, systems, or networks. This is not to say that facilities which do not reach these thresholds are not important or do not provide essential services, but there needs to be a justifiable "line in the sand" that delineates between what is critical to the Commonwealth and what may be critical to counties or other local jurisdictions. This will allow the Commonwealth to best allocate its limited resources in the most efficient and justifiable way possible. On the federal level, this had previously been accomplished for most sectors through its implementation of the Tier 1-2 Data Call, which asks states to provide DHS with an annual list of facilities that meet federal standards. However, these metrics changed yearly, and have now become based on consequence-based criticality rather than on quantifiable metrics. It has, therefore, become essential for the Commonwealth to develop its own tool for assessing criticality, so that an accurate list of its CIKR can be generated.

Likewise, specific tools also need to be developed to assess the risk associated with the identified CIKR. In fact, this objective requires the creation of measures to define the quantifiable values attributed to each of the three variables that make up the risk formula, as well as a way to synthesize those three values into an overall assessment of that facility's risk. To ascertain a value for vulnerability, OHS originally developed the concept of the SPP. This program was designed to consist of a vulnerability assessment that measured administrative-personnel issues, physical security measures, systems vulnerability and financial viability; and would have provided each facility with a risk mitigation strategy that included best practices and options for improving their posture. And, because it would have been virtually impossible to perform such a comprehensive assessment at every facility state-wide, the concept of a shorter Self Vulnerability Checklist was also developed to gather relevant data about each facility. However, development of the SPP and the Self Vulnerability Checklist concepts ceased after the installation of the new Homeland Security Organizational Structure on November 1, 2009. These programs—or something very similar—need to resume if the Commonwealth has any desire to analyze the risk associated with its numerous CIKR.

To obtain a value for the threat variable, there must be a method of synthesizing current intelligence into a measure that can compare the relative adversarial intent, capability and probability of occurrence across all of the planning scenarios, and across all of the infrastructure sectors. To address this, OHS developed a formula using the average probability of each planning scenario occurring at a particular facility combined with a numerical value representing the rank of its sector's perceived threat as deduced through a

constant interpretation of current intelligence. Subsequently, it became necessary to use an information fusion center, or similar entity, which had the ability to analyze current intelligence and synthesize such information into those inputs required by OHS. Formerly, OHS was unable to complete this task because of the absence of a state-wide fusion center and because PSP was unable to disseminate any information they perceived to be part of an ongoing investigation.[10] However, with the move by the Corbett Administration to co-locate OHS with PSP, the opportunity now exists for OHS to utilize the Pennsylvania Criminal Intelligence Center (PaCIC) to complete this task.[11] Though not a true fusion center, PaCIC nonetheless has the staffing and intelligence gathering capabilities to provide OHS with the direct intelligence it needs to develop a useful value for the threat variable.

The value for the consequence variable, on the other hand, is much simpler to obtain. As has been noted previously, OHS developed a formula that considered the impacts caused by the total loss or prolonged disruption of a particular facility, including the impacts on human health, economic activity, the ability of the government to continue delivering essential services, and the psychology of the populace. Based on separate 1-5 scales created for each type of impact with the help of the SSWG, the overall value for consequence represented the average of these scores for each facility.

Once all three variables have a justifiable measure, another tool must be employed that combines their values into an overall measure of risk. To accomplish this, OHS developed an algorithm that weighted each respective variable according to its relative importance, and then added those resulting scores together to determine the overall risk. To keep the resulting risk scores in an easily comparable 1-10 format, this formula used a value-added method to determine each weight as a fraction. For instance, the values for vulnerability and consequence were to be multiplied by 1/4, while the value for threat—because it is the most important—would have been multiplied by a factor of 1/2.

By comparing these risk scores to the identified gaps in the capabilities of each region or county, a risk profile for each CIKR could have been generated. This would have enabled OHS to develop funding priorities that efficiently mitigated those gaps using whatever limited resources were available to the Commonwealth. To accomplish this, though, there must be a mechanism through which potential HSGP investments in infrastructure protection can be prioritized. For example, such a mechanism could be a comprehensive database program that can analyze the information collected for each CIKR, and determine

[10] For these purposes, PSP utilizes the Criminal History Record Information Act (CHRIA), identified as 18 Pa. C.S.A. Section 9101 et seq., which limits the type of criminal justice information that may be disseminated to the public.

[11] According to PSP, PaCIC provides Pennsylvania's law enforcement community with 24/7/365 access to law enforcement information, and is designed to assist local, state, and federal law enforcement agencies with the prevention of crime and terrorism.

which ones are the most at-risk by comparing each site's risk score to the ability of its local first responders to respond to, and recover from, an incident at that facility. It must also be able to perform this function on an ever-changing basis because new and updated information is continuously collected and disseminated. But such a program has not yet been developed, and the Commonwealth is instead using a sub-optimal formula for the allocation of HSGP funding that does not consider the associated risk of the Commonwealth's CIKR. Other tools, such as DHS' C/ACAMS[12], can be used to store such information, but like most OTS products of its kind, it does not provide OHS with the ability to properly prioritize funding initiatives based on Pennsylvania's unique formulation of risk. However, using such a program may represent a stop-gap measure until a more comprehensive database program can be developed.

Because of the termination of the SPP project, the development of protection strategies would have been extremely difficult, if not impossible to attain under the previous Homeland Security Organizational Structure. This objective requires the use of the tools missing from the preceding ones, as without a way to gauge common vulnerabilities there will be no way to synthesize such information into strategies to mitigate them. However, by co-locating OHS with PSP, it now becomes possible for OHS to complete this objective. Whether by giving OHS the administrative support it needs to complete work on the SPP, or by allowing the office to contract out this objective to a third party that has both the subject matter expertise and the "boots-on-the-ground" resources necessary, it is imperative that this objective not fall by the wayside under the new structure. And, with the additional staffing resources available by co-locating OHS with PaCIC, it is certainly possible to develop sector-specific and/or Commonwealth-wide risk mitigation strategies without taking Commonwealth employees away from their regular duties for a significant amount of time.

Measuring the effectiveness of the state's Infrastructure Protection program can be accomplished relatively easily once the preceding objectives are attained. Since the reduction in risk must be measured by the mitigation of identified gaps in the capabilities of local first responders to effectively respond to and recover from an all-hazards incident, PEMA's annual capability assessment of the Regional Task Forces should be able to serve this task extremely well. If, for example, the program is effective, the funding allocated to the task forces will show an improvement in their capability scores in the following year's assessment. However, pursuant to the issues with the collected data in the past, it may also be necessary to develop a system of periodic audits of task force expenditures to ensure

[12] C/ACAMS refers to the Constellation/Automated Critical Asset Management System, which was designed as a Web-based platform that helps state and local governments build critical CIKR protection programs in their local jurisdictions according to DHS-defined norms. More information about this program can be found at http://www.dhs.gov/files/programs/gc_1190729724456.shtm.

that HSGP funding is being dispersed effectively to the proper first responder organizations.

6.0 Conclusion

With the reorganization of the Infrastructure Protection mission on November 22, 2011, many of the objectives discussed above may finally come to fruition. Without the move to PSP, it was highly unlikely that the two individuals who were tasked with completing them would have been able to do so without significant assistance from such extra-institutional entities as the Regional Task Forces, other state agencies, the private sector, and other industry or academic organizations. And, because none of these groups has a codified stake in the Infrastructure Protection Mission, it would have been extremely difficult to garner and sustain their support in the face of divergent responsibilities without significant changes to current legislation.

However, by co-locating OHS with PSP, it is apparent that the Corbett Administration has recognized that Infrastructure Protection is an extremely important duty within the Homeland Security spectrum of activities. As such, it is imperative that the Administration allow OHS to obtain those tools that would automate the processes outlined above, thereby enhancing its ability to complete the Infrastructure Protection mission. Currently, the Commonwealth is at a severe disadvantage without them, but the opportunity now exists for OHS to finally gain the support it has lacked since its inception ten years ago.

Though only time will tell whether or not the organizational shift will accomplish these goals, it is apparent that the Administration has come to the realization that changes to the Homeland Security Organizational Structure were needed in order to carry out its responsibilities to the citizens of Pennsylvania. Nevertheless, this move only represents the first step, and the Corbett Administration must now follow through on its decision by allowing OHS to develop the tools it needs to identify, assess, and, most importantly, reduce the risk associated with Pennsylvania's CIKR.

About the Author

Eli Gilman is a Research Associate for FPRI's Center on Terrorism and Counterterrorism. He served in various positions from 2007 to 2009 with the Pennsylvania Office of Homeland Security, in which his primary focus was the development and implementation of the Commonwealth's Critical Infrastructure Protection Program. Currently pursuing a Masters Degree in Public Policy at Drexel University, he received his B.A. in Political Science from George Washington University.

Foreign Policy Research Institute

Walter A. McDougall
Chair, Board of Advisors

Alan H. Luxenberg
Acting President

BOARD OF TRUSTEES

Robert L. Freedman
Chairman

Samuel J. Savitz
Dr. John M. Templeton, Jr.
Hon. Dov S. Zakheim
Vice Chairs

Hon. John Hillen
Treasurer

Gwen Borowsky
Richard P. Brown, Jr.
W.W. Keen Butcher
Elise W. Carr
Robert E. Carr
Ahmed Charai
William L. Conrad
Devon Cross
Gerard Cuddy
Peter Dachowski
Edward M. Dunham, Jr.
Robert A. Fox
James H. Gately
Susan H. Goldberg
Charles B. Grace, Jr.
Jack O. Greenberg, M.D.
John R. Haines
Graham Humes
Hon. John F. Lehman
Richard B. Lieb
David Lucterhand
David Marshall
Rocco L. Martino
Robert McLean
Ronald J. Naples
Marshall W. Pagon
James M. Papada III
James E. Phillips
John W. Piasecki
Alan L. Reed
Eileen Rosenau
J. G. Rubenstein
Lionel Savadove
Hon. James Saxton
Adele K. Schaeffer
Edward L. Snitzer
Bruce D. Wietlisbach

BOARD OF ADVISORS

Paul Bracken
Michael S. Doran
Thomas V. Draude
Charles J. Dunlap, Jr.
David Eisenhower
Adam M. Garfinkle
Frank G. Hoffman
Robert D. Kaplan
Bernard Lewis
Walter A. McDougall
Robert C. McFarlane
William H. McNeill
Kori Schake
Murray Weidenbaum

Foreign Policy Research Institute
1528 Walnut Street, Suite 610
Philadelphia, PA 19102
(215) 732-3774
www.fpri.org