Foreign Policy Research Institute

E-Notes

A Catalyst for Ideas | *Distributed via Email and Posted at www.fpri.org* | **December 2011**

RISK AND RE-ORG: INFRASTRUCTURE PROTECTION IN THE COMMONWEALTH OF PENNSYLVANIA

EXECUTIVE SUMMARY

By Eli S. Gilman

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 Master's Degree in Public Policy at Drexel University, he received his B.A. in Political Science from George Washington University.

Editor's Note: ***With support from the Commonwealth of Pennsylvania, FPRI's Center of Terrorism and Counterterrorism examined the Commonwealth's overall state of readiness, as well as the state's success and failures in using Homeland Security resources. This E-Note is an Executive Summary of the Center's research. Read the full monograph at http://www.fpri.org/pubs/2011/201112.gilman.pahomelandsecurity.pdf.***

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 (hereafter referred to simply as critical infrastructure).

Since the events of September 11, 2001, homeland security has become one of the most important responsibilities at all levels of government. In the Commonwealth of Pennsylvania, however, systemic inefficiencies arose that precluded progress under the former governance structure. In particular, these inefficiencies stifled the ability of the state to perform virtually any of the Critical Infrastructure Protection duties 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 9/11, the results mostly exacerbated existing issues rather than instilling any long-term solutions.

Now, tough, with OHS being co-located with PSP, the opportunity exists for such solutions to come about. This move will enable better coordination between the intelligence gathering operations at PSP and the intelligence dissemination functions of OHS, and position OHS to offer greater protection of Pennsylvania's critical infrastructure.

Though it is apparent that the current administration has recognized that OHS would never have been able to fulfill its objectives under the former governance structure, it is vitally important to complete a thorough analysis of the shortfalls that have existed in the Commonwealth's Infrastructure Protection mission since 9/11 in order to ensure that they are not repeated under the new structure.

THE ORGANIZATION OF INFRASTRUCTURE PROTECTION IN PENNSYLVANIA

At the state level, successfully implementing Infrastructure Protection is dependent upon the unique socio-political characteristics and governance structures that define a given state's institutional culture. In the Commonwealth, Homeland Security functions have been 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 PSP; protection activities by OHS; and response and recovery activities by PEMA. In addition, because of the wide-ranging nature of Homeland Security activities, several other state agencies have jurisdiction over specific policy areas and, therefore, play a significant role in all four of the mission areas listed above. 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.

Following the institutional realignment that took place after 9/11, state and local governments were asked to play a larger role in homeland security through enhanced collaboration with the federal government, the fusion of intelligence information and a new focus on identifying and protecting critical infrastructure.[1] In Pennsylvania, 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.[2]

Over the next decade, lessons gained from subsequent events, such as the responses to Hurricanes Rita and Katrina, also altered the Homeland Security Organizational Structure nation-wide. However, no event shaped the Commonwealth's direction regarding such activities more than its 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 state's response to the storm. The result was hundreds of motorists stranded on Pennsylvania's highways for hours as state officials tried to clear the more than 50-mile traffic jam that developed. The resulting study, conducted to assess the current Emergency Management Organizational Structure, proposed many changes designed to increase collaboration, encourage pre-defined disaster response leadership positions, and institute a new Homeland Security Organizational Structure that would bring the Infrastructure Protection responsibilities under the PEMA Director.[3]

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 the Health and Safety Code (Title 35) and the creation of the new Department. However, almost two years and an administration later, neither of these items ever occurred. Likewise, Infrastructure Protection played nearly no role underneath this 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 was said at the time 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 critical infrastructure.

Nevertheless, this may all change with the announcement by Governor Corbett that OHS would now be moving to PSP. 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 may 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.

---

[1] 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.

[2] 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.

[3] This report was conducted by the James Lee Witt Associates, which 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, A_Report_Final.pdf."

RISK-MITIGATION OBJECTIVES

In theory, executing any successful Infrastructure Protection program requires first reducing the overall risk to its critical infrastructure and key resources. And because federal guidelines require that this must be measured by how local first responder capabilities have been enhanced, state-centered risk-mitigation strategies must deter threats, reduce vulnerabilities and mitigate potential consequences by ensuring that all allowable funding is dispersed in the most effective and efficient manner. Thus, a measured reduction in risk can only occur by ensuring that this funding is allocated in accordance with some measure of calculated risk that both identifies and prioritizes gaps in target capabilities, and which can be used universally across all sectors. In addition, such a program's successful implementation requires the sharing of complete, accurate, and reliable critical infrastructure information among other governmental and private sector partners.[4] This will enable situational awareness and enhance emergency response planning by both the private sector and first responders. Achieving this will also give each entity the capability to assess risk on their own and execute the necessary risk-mitigation plans.

Risk mitigation, thus, must be derived through a continuous cycle of six objectives: setting 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. First, 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 critical infrastructure owners and operators should aim.

The second objective requires identifying 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 consistent, structured terminology allows for designating critical infrastructure 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.[5] Once this has been accomplished, sector-specific criteria must be developed to assess the criticality of each site using a standard, applicable method. Additionally, because critical infrastructure and their elements can be described in different ways, such classification needs to be consistent across varying levels of government. Failure to do so could result in conflicting terminologies that impede communication, and could obstruct the decision-making process during an emergency.

Once the critical infrastructure have been identified, it is necessary to determine the overall risk that can be attributed to each site on a universally consistent basis, thereby enabling comparison across sector and jurisdictional boundaries. To accomplish this, a formula must be developed that accurately depicts the nature of risk as a function of a site's vulnerability to disruption from an all-hazards incident, the perceived threat against it, and the consequences that such a disruption is likely to cause. And because such a formula is inherently based upon subjective analyses, it must also be convertible to 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 critical infrastructure to determine which sites are most at risk. However, this does not provide a complete picture because the existing capabilities to mitigate the perceived risk have not yet been identified. Once this is achieved, a risk profile can be generated showing 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 critical infrastructure. 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.

Based on the risk profiles generated, it becomes possible to prioritize efforts in funding first responder activities, equipment,

---

[4] 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.

[5] For the purposes of this objective, the DHS Infrastructure Taxonomy is used to classify critical infrastructure 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.

planning efforts, and exercises. However, it is important to remember that prioritization is a dynamic process. New threat factors affecting each sector of critical infrastructure surface daily and other, newly collected information regarding site-specific vulnerabilities or regional capabilities can dramatically affect which capability enhancements are most needed. Therefore, the prioritization methodology must be able to account for changes to the inputted information such that wholesale adjustments to the methodology are unnecessary.

The complete protection of critical infrastructure will be the most difficult objective to attain. With over 85 percent of all critical infrastructure residing in the private sector, enhancing the response capabilities of first responders through available funding will only accomplish so much. Gaining the participation and support of the critical infrastructure owner/operators is, therefore, paramount to the success of this objective. This is the case because the best efforts to identify, prioritize, and fund the needs of first responders are meaningless unless the owner/operator feels the same obligation to invest in their own protection efforts and security. While legal restrictions prohibit the state from providing physical security enhancements to these private sites, the Commonwealth can recommend resiliency strategies by providing opportunities to share lessons learned and best practices on an industry-wide basis, and by providing options for consideration—which are in no way binding—that can, at the very least, enable the critical infrastructure owner/operator to gain a better understanding of his or her facility's shortcomings. Critical infrastructure owner/operators can then perform their own cost/benefit analyses to determine what security enhancements should be made without increasing liability.

Like the prioritization process discussed above, measuring the effectiveness of Infrastructure Protection activities is also an ongoing effort. A mechanism is needed to perform periodic capability assessments, which identify improvements among the necessary target capabilities. Not only is this simply 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. This will, in-turn, drive future funding strategies. As the relative success of this entire program is evaluated, it may become necessary to revise it accordingly to better facilitate the overarching goals of Infrastructure Protection.

IS PENNSYLVANIA MEETING ITS OBJECTIVES?

Originally, OHS set up several advisory councils and working groups comprised of government officials, private sector representatives and local first responders in order to include all of their viewpoints on potential Homeland Security issues. However, with the institutional realignment that took place in 2009, these groups were abolished, and OHS had to rely more heavily on other state agencies at the expense of the private sector partners whose industries those agencies regulate.

Before this occurred, though, OHS was able to tap its various partners to help develop the overarching security goals that determined the direction of future Infrastructure Protection objectives. Specifically, these partners helped to develop Pennsylvania-specific planning scenarios that illustrate the most probable worst-case situations to which the Commonwealth and its critical infrastructure must be resilient. These scenarios, while taken from the original 15 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.[6]

The identification of critical infrastructure, on the other hand, was a much more laborious—and ultimately frustrating—process. While the classification methodology provided by the Department of Homeland Security in the Infrastructure Taxonomy is useful in determining what an asset is once it has been identified, the lack of a consistent definition of what constitutes criticality has deterred concretely identifying the Commonwealth's critical infrastructure. The Commonwealth, therefore, used a more subjective method to identify its critical infrastructure. It relied on each agency's institutional knowledge and a "boots on the ground" approach from its local government partners. Certainly, this method has produced a comprehensive list of the Commonwealth's critical infrastructure, but without a clear definition of what constitutes criticality, such a list will always be sub-optimal.

Conversely, the assessment of risk was a much more successful endeavor. As noted earlier, risk can be defined as a function of vulnerability, threat and consequence. With the help of its partners, OHS was able to develop basic measures for all three of these variables. By using a mathematical algorithm weighted by current threats, it synthesized these measures into a relative value of risk that can be compared to that of each identified asset. In the OHS algorithm, the threat value obtained through this measure is the most heavily weighted because if there is no threat, the vulnerabilities and consequences become far less significant.

By completing these assessments Commonwealth-wide, OHS would have been able to prioritize all potential investments so as to mitigate identified gaps in the capabilities of local first responders by determining the set of most at-risk critical infrastructure, and then comparing that list to identified shortcomings at the local, county and regional levels to determine

[6] 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

funding priorities. Unfortunately, due to insufficient tools and resources at the state level, the Commonwealth was not able to do this. A comprehensive critical infrastructure database program, for example, would have been able to perform this function on an ever-changing basis. However, due to 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 critical infrastructure within each region to determine local allocations of each year's funding. While this measure does prioritize funding initiatives based—at least in part—on identified critical infrastructure, it does not allow for any prioritization based on the associated risk attributed to them. Developing the aforementioned database program is, therefore, essential to the successful completion of this objective, and 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 critical infrastructure, let alone the risk attributable to each sector/industry or, ultimately, the Commonwealth over all. In order to accomplish this, OHS began developing what it called, the Site Protection Plan Program. This program was designed to elicit site-specific information through the use of the comprehensive vulnerability assessment required by the third objective. Comparison of these protection plans would, therefore, 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 not only to each sector, but Commonwealth-wide. Once OHS was placed under the direction of PEMA, though, work on the Site Protection Plan was curtailed, leaving this objective unfulfilled and virtually unattainable. However, by co-locating OHS with PSP, it now becomes possible for OHS to complete this task. Whether by giving OHS the administrative support it needs to complete work on the Site Protection Plan, or by allowing the office to contract out this function to a third party, it is imperative that this objective not fall by the wayside under the new structure.

Finally, unless the gaps prohibiting the completion of the preceding objectives are bridged, there is no way to effectively measure reduced risk to the Commonwealth's critical infrastructure, or to assess the overall viability of Pennsylvania's Infrastructure Protection Program as a whole. Previously, PEMA relied on systematic audits of expenditures to see if they simply fell in line with the State's overarching strategy, and with the individual spending plans developed prior to the disbursement of federal funds. PEMA also conducted a state-wide capability assessment to identify the baseline capabilities present across the Commonwealth, but this assessment was severely inadequate because insufficient information was collected regarding county and local level capabilities, and because evaluators were asked to reduce their initial estimates to show greater improvement in subsequent evaluations. As such, new methods and tools must be developed to better capture this data and to properly analyze any reduction of risk to the Commonwealth's critical infrastructure.

INFRASTRUCTURE PROTECTION MOVING FORWARD

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.