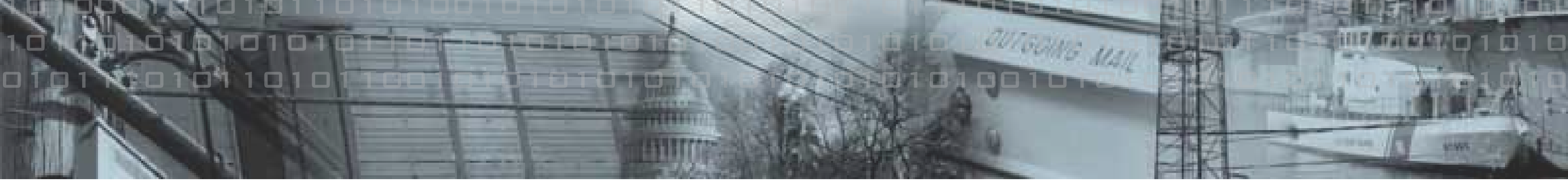

THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 11 NUMBER 8

FEBRUARY 2013
POLICY

In this month's issue of *The CIP Report* we focus on current policy issues and initiatives facing the new administration.

GEORGE MASON UNIVERSITY

School of Law

CENTER
for
INFRASTRUCTURE PROTECTION
and
HOMELAND SECURITY

First, CRA Executive Vice President and former DHS Assistant Secretary for Infrastructure Protection Robert Stephan examines the road ahead for critical infrastructure protection and resilience, highlighting key focus areas and initiatives. Then, Evan Wolff, Partner and Director of Homeland Security Practice at Hunton and Williams, and law student Emily Barber, give an overview of several critical infrastructure protection policy changes likely to occur in the second Obama administration. International law Professor Jeremy Rabkin next discusses new policy on cybersecurity offensive tactics, particularly regarding preemptive strikes. Finally, Christopher Krebs of Obsidian Analysis gives an in-depth examination of the Chemical Facility and Anti-Terrorism Standards Program.

This month's *Legal Insights* looks at the evolution of preemption—from a concept to a national policy—and asks what this means in light of emerging threats.

We would like to take this opportunity to thank the contributors to 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

EDITORIAL STAFF

EDITOR
Kendal Smith

STAFF WRITER
Manal Farooq

JMU COORDINATORS
Ben Delp
Ken Newbold

PUBLISHER
Melanie Gutmann

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

Follow us on Twitter here
Like us on Facebook here

Laying Out Next Steps for Critical Infrastructure Protection and Resilience

by Robert B. Stephan, Executive Vice President, CRA, Inc.

The Challenge: Protecting and Enhancing the Resilience of Critical Infrastructure in the 21st Century Risk Environment

The global environment affecting our critical infrastructure comprises a highly diverse and complex mix of manmade and naturally occurring threats and hazards. These threats are not hypothetical in nature—they are real, unforgiving, and deadly. On the manmade front, they include nation-states operating outside of international norms, international terrorists, domestic extremists, malicious cyber actors, and technology failures often compounded by catastrophic human error. On the natural disaster front, they include things like the Great East Japan Earthquake, Tsunami, and Fukushima Daiichi nuclear reactor disaster, and more recently, Super Storm Sandy—events which spawn over-sized impacts relative to densely packed population centers and the lifeline infrastructures that support them. Add the possibility of a global pandemic and the growing effects of global climate change, and the forecast for the future threat/hazard environment becomes even more worrisome.

From the perspective of other key elements of risk, our critical infrastructure sectors are increasingly vulnerable due to the nature of their physical operating environments, functional dependencies and interdependencies, and distributed cyber connections. These vulnerabilities are compounded by "just-in-time" product and service delivery tied to a highly interconnected global economy and international supply chains, where a single "blip" can have disproportionately negative impacts system-wide, and in short order. As evidenced in the wake of Super Storm Sandy's landfall, the complex scope of dependencies and interdependencies that cuts across our critical infrastructure sectors makes our core population centers and national economy very fragile in the context of complex disasters.

To appropriately manage risk in light of these complexities, government and industry partners have worked closely together since the 9/11 attacks to develop and implement a focused, national approach to critical infrastructure protection and resilience, including policies, analytical capabilities, sector plans and partnerships, coordinating structures, and information sharing mechanisms. This approach balances resilience with risk-informed prevention, protection, and preparedness activities to allow us to address our most serious critical infrastructure risks, now and in the future. Looking ahead, successes achieved to date will be reinforced through the comprehensive "Whole Community" focus under the new national preparedness guidance provided in Presidential Policy Directive 8 (PPD-8).

Complicating the above approach, however, is the fact that the government and private-sector entities that share responsibility for critical infrastructure protection and resilience represent a varied mix of authorities, capabilities, and increasingly scarce resources. These actors also have unique concerns arising from the functional dependencies and interdependencies that characterize the infrastructure of concern under their individual purviews. These diverse factors result in very different outlooks and needs relative to the protection and resilience of our critical infrastructure and related supply chains—particularly those that involve dynamic interaction across geopolitical and sector boundaries. Successful navigation of this extremely complex environment is only possible through a continued "team effort" at the national, regional, and local levels. That is, through a collective public-private approach to preparedness, assessment of risk, planning, and risk mitigation.

(Continued on Page 3)

(Continued from Page 2)

Strategic Imperatives

Looking ahead, the critical infrastructure protection and resilience "national team" must work very closely together—within the context of a fragile fiscal environment— to achieve three overarching strategic, all-threats/all-hazards imperatives:

1) Identify, protect, and make more resilient those infrastructure systems and assets assessed to be most critical nationally in terms of public health and safety, economic and national security, continuity of government and essential services, and public confidence considerations.

2) Provide timely warning and protect those infrastructure systems and assets that face a specific, imminent threat (manmade or naturally occurring), irrespective of national-level criticality.

3) Promote a collaborative environment in which to enhance the protection and resilience of other infrastructure systems and assets that may become higher risk over time or take on greater criticality than normal, based on the nature of a specific emergent threat situation.

Regarding the first imperative, we must focus maximum attention and resources—in the context of "steady-state" preparedness and planning—on those infrastructure elements for which the consequence of loss or disruption presents an unacceptably high risk based on nationally-derived criteria. We must also consider infrastructure that are "critical by association." Simply put, this means those systems/assets that are in close physical proximity to, and/or are functionally connected to, the system or asset of primary national level concern (e.g. primary sources of off-site power, water, communications, etc., for nuclear power plants and critical national defense production facilities). As such, this imperative puts a premium upon sophisticated geographic clustering, cross-sector dependencies/interdependencies, and physical-cyber infrastructure link analysis.

Regarding the second imperative, we must be prepared to protect an infrastructure system or asset at risk as a result of a specific, credible, and/or imminent threat or hazard situation, regardless of whether or not it is ranked "nationally critical." Meeting this imperative will require an expansive network of collaborative partnerships, public-private information sharing mechanisms, and physical/cyber protective "surge" capabilities, tailored to the nature of the threat/hazard at hand.

Finally, regarding the third imperative, it is essential that the "national team" include a very broad and diverse array of infrastructure owners/operators, first responders, public officials, emergency managers, regulators, and others who have a stake in critical infrastructure protection and resilience, both specifically and writ large. This stakeholder coalition must be representative of a much greater mix of infrastructure systems/assets than those which we deem "nationally" critical on a steady state basis or those that face a specific, imminent threat. This is important for two reasons: 1) the effectiveness of the critical infrastructure mission is a direct function of the number and diversity of concerned stakeholders engaged "in the fight" on a day-to-day basis, and 2) we can never fully predict what a terrorist adversary or Mother Nature may cause to become "nationally critical" outside our high-risk definitional parameters (e.g. elderly care facilities filling up with water and service stations with emergency generators on evacuation routes on Day 1 of Hurricane Katrina's landfall). This third pillar must include a focus on ways and means to promote and facilitate meaningful stakeholder engagement in critical infrastructure protection and resilience as a matter of course, lest we be outflanked by a wide range of threat/hazard vectors in any number of highly consequential ways.

Critical Infrastructure Protection Focus Areas & Initiatives

Getting our arms around the strategic imperatives outlined above will be no easy task, but a task nonetheless achievable as long as the "national team" stays the course. The focus areas presented below should be considered as key elements defining the path forward:

- *Systematically Focus Dependencies/ Interdependencies Analysis to Mitigate Our Greatest Risks.*

Over the past decade, the Federal government has invested vast resources in the development of an increasingly sophisticated infrastructure dependencies/ interdependencies analytical capability. This effort

(Continued on Page 12)

Critical Infrastructure Protection in the Second Obama Administration

by Emily A. Barber, J.D. Candidate, May 2013, George Mason University School of Law (GMU) and Evan D. Wolff, Adjunct Professor of Law, GMU, and Partner and Director, Homeland Security Practice, Hunton & Williams, LLP

In August 2012, a virus named Shamoon infected 30,000 computers and 1,000 servers owned by the Saudi Arabian State Oil Company, Saudi Aramaco, turning the company's computer screens blue and replacing crucial files with an image of a burning American flag.[1] Luckily, Shamoon only reached the company's computer systems. If it had reached the industrial control system, more than 30 percent of the Gulf's oil supply and 10 percent of the world's oil supply could have stopped.[2] One week later, a similar virus attacked RasGas of Qatar.[3] Secretary of Defense Leon Panetta called Shamoon "the most destructive attack that the private sector has seen to date."[4]

Our Nation's critical infrastructure has also been targeted by cyber terrorists. As the U.S. Government openly acknowledged, beginning in the spring of 2012, a cyber intrusion campaign was directed against the U.S. pipeline industry.[5] Secretary Panetta warned that the United States could face a cyber threat that goes beyond the energy industry, creating a "cyber Pearl Harbor."[6] This type of campaign, as well as the lessons learned from the devastating impacts of natural hazards like Hurricane Sandy and the National Capital Region Derecho storm, shows the importance of being prepared to protect all aspects of our Nation's critical infrastructure. The existing threats against U.S. industries have resulted in efforts by the U.S. Government to strengthen cybersecurity standards for critical infrastructure and to encourage owners of critical infrastructure to enhance their security practices. This paper discusses critical infrastructure protection policy changes that are likely to occur over the next four years of the Obama Administration, with a focus on the Department of Homeland Security's Chemical Facility Anti-Terrorism Standards, consideration of cybersecurity regulations for the pipeline industry, proposed regulations for ammonium nitrate, and other actions by the Executive branch pursuant to its Executive authorities.

Chemical Facility Anti-Terrorism Standards

DHS has statutory authority to regulate high-risk chemical facilities for security purposes.[7] The Chemical Facility Anti-Terrorism Standards (CFATS), codified at 6 C.F.R. Part 27, is the DHS regulation governing security at high-risk chemical facilities.[8] This regulation requires that facilities with designated quantities of "chemicals of interest" submit information to DHS in order to help DHS determine the risk status

(Continued on Page 5)

[1] Parmy Olson, "The Day A Computer Virus Came Close To Plugging Gulf Oil," FORBES, Nov. 9, 2012, available at http://www.forbes.com/sites/parmyolson/2012/11/09/the-day-a-computer-virus-came-close-to-plugging-gulf-oil/; Secretary of Defense Leon Panetta, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012) (transcript available at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136).

[2] Olson, *supra* note 1.

[3] *Id.*; Patrick Osgood, "Cyber attack takes Qatar's RasGas offline," ARABIANBUSINESS.COM, August 30, 2012, http://www.arabianbusiness.com/cyber-attack-takes-qatar-s-rasgas-offline-471345.html.

[4] Panetta, *supra* note 1.

[5] DEP'T. OF HOMELAND SEC., *ICS-CERT Monthly Monitor* (April 2012), available at http://www.hsdl.org/?view&did=714567.

[6] Panetta, *supra* note 1.

[7] Department of Homeland Security Appropriations Act, Pub. L. No. 109-295, § 550 (2007).

[8] Chemical Facility Anti-Terrorism Standards, 6 C.F.R. § 27 (2007).

(Continued from Page 4)

of each facility.[9] Facilities deemed by DHS to be high-risk must develop site security plans (SSPs) for DHS review and approval. The SSPs include risk-based performance standards (RBPS), including standards to secure a facility's cyber systems from attack.[10] The CFATS RBPS provide a flexible legal framework for securing high-risk facilities because they state the required results, but do not mandate a required compliance method. These types of standards are more flexible than prescriptive standards which the federal government has used for some other regulatory programs that state the required method for accomplishing the results.[11]

The 112th Congress extended DHS's authority under the CFATS program to regulate chemical facilities for security purposes through March 27, 2013, and President Obama requested an extension until October 4, 2013.[12] This request comes in light of press coverage highlighting the challenges and shortcomings of the CFATS program, including the time and resources required to build this program, and some of the external metrics, including DHS's pace in approving SSPs.[13] It is likely that, under the second Obama Administration, DHS will reflect on these issues, look at areas of improvement, and begin the process of revising the program. Issues that DHS is likely to consider include greater transparency in screening and regulatory analysis, increased use of security processes including vulnerability assessments and security plans that are more widely used by industry, impacts of the program on the cybersecurity of covered facilities, and use of third-party inspectors at covered facilities. Additionally, as part of this process, the Administration may consider whether to apply the CFATS model of risk-based performance standards to cybersecurity because it would allow individual companies and industries to tailor security plans based on risk to a particular system.

Pipeline Industry Guidelines

Pipeline safety and security issues could also be an area of interest and review during this Administration. Specifically, the Transportation Security Administration's (TSA's) authority, based on the 9/11 Act of 2004, allows for a review of the security issues impacting this sector. To date, the TSA initiated an industry-wide process to bring the pipeline sector together to voluntarily develop cybersecurity guidance and best practices. The pipeline industry has used these guidelines to establish security requirements in the management of security and new construction. This process is widely seen as a positive example of self-regulatory efforts to develop security guidance and a model of public-private partnership. The pipeline industry has long been regulated by performance-based standards rather than prescriptive rules, and such an approach is believed by many in the sector to be well-suited to cybersecurity issues. As the pipeline industry continues to focus on cybersecurity issues and concerns regarding liability risks, the industry is likely to continue to evaluate current best practices and standards. Moreover, there remains the possibility that the second Obama Administration may seek to rely upon TSA's existing authorities to issue regulations on pipeline security to address the increased cyber risks to U.S. pipelines.

Ammonium Nitrate Proposed Regulations

In the second Obama Administration, DHS will likely increase its focus on implementing an ammonium nitrate regulatory program. DHS issued a proposed rule in August 2011 to regulate the sale and transfer of ammonium nitrate aimed at preventing its use in an act of terrorism.[14] DHS is primarily concerned with the use of

(Continued on Page 14)

[9] *Id.*

[10] DEP'T OF HOMELAND SEC., OFFICE OF INFRASTRUCTURE PROTECTION, *Risk Based Performance Standards Guidance: Chemical Facility Security Anti-Terrorism Standards* 71 (2009), available at http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf.

[11] Dana Shea, Cong. Research Serv., R41642, *Chemical Facility Security: Issues and Options for the 112th Congress* (2012).

[12] *Id.* at 1.

[13] *Id.* at 7; Jessica Zucherman, *Chemical Security in the U.S.: CFATS Regulations Too Complex, Overly Burdensome*, THE HERITAGE FOUND., Aug. 14, 2012, http://www.heritage.org/research/reports/2012/08/chemical-security-in-the-us-cfats-regulations-too-complex-overly-burdensome.

[14] Ammonium Nitrate Security Program, 76 Fed. Reg. 149 (proposed Aug. 3, 2011) (to be codified at 6 C.F.R. § 31).

New Obama Policy on Cyber Offensives- A Little At A Time

by Jeremy Rabkin, George Mason University School of Law

The Obama administration has decided that it might be appropriate to launch a preemptive cyber strike "if the United States detects credible evidence of a major digital attack looming from abroad." At least that is what unnamed sources within the administration recently confided to *The New York Times*.[1]

This latest policy position seems to mark a new stage in the development of American cyber policy. But a great many questions remain unresolved, even on the administration's view of the relevant legal constraints.

The questions are not mere niceties of nomenclature or procedure. The administration seems determined to embark on more vigorous cyber initiatives. Leaks to *The Washington Post*, a few weeks earlier, indicated that the Obama administration plans a five-fold increase in the personnel allocated to the Defense Department's Cyber Command, even while budgets for other Pentagon programs are sharply reduced.[2] But there has been a long-running debate about how and when to approve offensive operations in cyberspace.

The 2012 Defense Authorization Act (approved in December 2011) "affirm[ed]" that "the Department of Defense has the capability and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests." But the same provision insisted that such "operations" are "subject to (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution."[3]

A few months later, the White House leaked to *The New York Times* that President Obama had, starting in 2009, authorized secret cyber attacks aimed at disrupting Iran's nuclear program.[4] A few months later, Harold Koh, Legal Adviser at the Department of State, gave a presentation at an inter-agency conference, affirming that cyber attacks should be governed by the international law of armed conflict (LOAC).[5] But Koh did not provide much detail about how the Obama administration interprets the LOAC.

The first and most obvious question is when resort to force is justified. The UN Charter acknowledges that all states have an "inherent right" of self-defense "if an armed attack occurs."[6] Could a cyber attack be considered an "armed attack"? Koh argued that cyber attacks which caused "death, injury or significant destruction would be viewed as a use of force"—justifying a wide range of measures in self-defense.

The recent leaks indicate the Obama administration has now taken the next step and asserted a right to act in self-defense when a major cyber attack is threatened, even if it has not yet occurred. That would be consistent with the view of most scholars and most governments, that in authorizing actions in self-defense, the UN Charter implicitly authorizes preemptive measures against imminent attacks. It would be consistent with warnings that a major cyber attack, targeting electric grids or other critical infrastructure, could have a crippling effect on the whole U.S. economy. It would be consistent with the theory on which the Obama administration

(Continued on Page 7)

[1] David Sanger and Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes," Feb. 4, 2013.

[2] Ellen Nakashima, "Pentagon to boost cybersecurity force," Jan. 27, 2013.

[3] Sec. 954.

[4] David Sanger, "Obama ordered sped up wave of cyberattacks against Iran," June 1, 2012.

[5] "International Law in Cyberspace," Remarks at USCYBERCOM Inter-agency Legal Conference, Sept. 18, 2012.

[6] Art. 51.

(Continued from Page 6)

has authorized drone strikes against terrorists in foreign countries.

But applying this theory to cyber attacks raises a great many new issues. The Obama administration claims that drone strikes on terrorists remain authorized by the authorization-of-force resolution enacted by Congress in the wake of the 9/11 attacks in 2001. The theory there is that today's jihadis are part of the same "enemy" that attacked the World Trade Center. Could Congress provide open-ended authorization to respond to cyber threats—whether they come from Russia, China, Iran or some other hostile state? Or would the administration need to seek congressional approval for each separate cyber operation, involving attacks on foreign countries?

If the administration has to justify separate interventions in cyberspace, it may have great difficulty making its case. We already have intelligence reports indicating preparations among various unfriendly states (and some friendly ones) for large-scale offensive cyber operations. With terrorists, it is easy to assume that a training base or a network will soon be used to launch a strike. With a state, we cannot assume that developing a capacity indicates a readiness to use it—let alone a readiness to use it imminently. After all, the United States is developing offensive capacities, while insisting that it will only use them for defensive purposes.

Even if the President is given convincing evidence of an impending cyber attack, would he feel bound to share this information with Congress? If not, how can there be meaningful congressional control on the launching of cyber offensives? Or would the President feel entitled to conduct a large scale cyber operation in secret? We don't conceal that drone strikes on terrorists are the work of the United States. But the United States did not acknowledge its responsibility for cyber disruptions of the Iranian nuclear program until years later (and then only in leaked stories to favored journalists). If another government charged the United States with engaging in cyber attacks, would we try to deny our actions or defend them openly if challenged, say, at the UN Security Council? Even if we were highly confident of our intelligence, would we want to disclose our sources in a public debate at the UN?

These difficulties might be avoided by claiming that a preemptive attack on a computer network in another country—disabling selected servers but injuring no human beings—should not be considered "force" so not covered, after all, by the rules that apply to armed conflict. But if we think of our responses that way, we might have to think of incoming attacks in the same category—crimes, perhaps, but not acts of war justifying emphatic responses. If the law of armed conflict does not apply, we might give ourselves more room to ignore the admonitions of the International Red Cross (and many scholars) that even cyber attacks must, like other military attacks, be limited to proper military targets and not be directed at civilian infrastructure. That would leave fewer legal doubts about attacking computer networks in other countries without agonizing about how to classify them (was the Iranian nuclear program "civilian," as claimed by the Iranian government?). But it would make it harder to raise angry protests about attacks on "civilian" targets in the United States. Harold Koh's speech last fall suggested that the administration was, in general, still attached to the theory that LOAC rules apply to cyber attacks.

A year ago, Stewart Baker, former general counsel to the National Security Agency, warned that government lawyers were "tying themselves in knots of legalese… to prevent the Pentagon from launching cyber attacks."[7] The current leaks suggest the Obama team is struggling to loosen those legal "knots"—but not yet prepared to cut them with decisive strokes. ❖

[7] "Lawyers are crippling America's ability to defend against cyberwar," *Foreign Policy*, Sept. 30, 2011.

Priorities for the Chemical Facility Anti-Terrorism Standards (CFATS) Program

by Christopher C. Krebs, Principal, Obsidian Analysis, Inc.*

As Secretary Janet Napolitano embarks on her second term at the helm of DHS, she has the opportunity to focus attention on a variety of programs that have been buried over the past few years by higher profile issues (such as cybersecurity, border control, and aviation security). The Chemical Facility Anti-Terrorism Standards (CFATS) program, residing within the Office of Infrastructure Protection (IP) arm of the National Protection and Programs Directorate (NPPD), is a perfect example of a DHS program that potentially poses a substantial amount of risk to the Secretary if not implemented properly.

By way of background, CFATS became effective in December of 2007 with the release of the list of Chemicals of Interest (COI) and associated quantities subject to regulatory authority. The program required chemical companies in possession of those chemicals to submit to a series of screening mechanisms, including initial consequence screening, vulnerability assessment, and finally development of a security plan, all aiming to identify those facilities that posed the highest security risk. Notwithstanding the internal report leaked in December of 2011 detailing the program's management and implementation shortcomings—and the subsequent congressional scrutiny of the program stemming from the report and ensuing leadership changes in the Infrastructure Security Compliance Division (ISCD)—CFATS has maintained a relatively low profile on the national scene.

In order to continue to stay out of the spotlight, and most importantly to continue to reduce risk and enhance security at our Nation's chemical facilities, the Secretary and DHS should focus on addressing the most pressing challenges across the CFATS program, ranging from leadership, compliance determinations, and full program implementation. As 2013 marks the fifth year of the program, it is an opportune time to review the program's progress and identify those areas for improvement and lessons learned.

The Importance of Stable Leadership

Organizationally, the CFATS program has suffered from a fairly dynamic leadership situation since its inception in late 2006. ISCD Directors and Deputy Directors have come and gone in the intervening time period with varying degrees of success and organizational impact or influence. Often, Deputy Directors would step up and act in place of the outgoing Directors, and then those Directors themselves would depart. The current Director, David Wulf, certainly fits at least the first part of that trend. Director Wulf joined the program in July of 2011 as the Deputy Director. He later assumed the Director role in 2012. Wulf was recently joined in the ISCD Front Office by new Deputy Director Scott Breor, the former Deputy Director of the now defunct Office of Risk Management and Analysis. Breor brings immediate risk analysis and management qualifications and credibility, a much needed attribute following the tier level miscalculation reported in 2011.[1]

The years of instability in the CFATS leadership structure have contributed to several detrimental results that are currently manifesting both internal and external to the program. Internally, the constant change in the front office has undermined staff morale, as many of the program officers seemingly have to redirect program priorities on a regular basis. Further, those program officers tend to keep their "Smart Books" handy, as they never know when a new round of "in briefings" for the next director might be necessary.

(Continued on Page 9)

[1] *A Survey of CFATS Progress in Securing the Chemical Sector*, American Chemistry Council, Sept. 6, 2011, pg. 12.

(Continued from Page 8)

Externally, as with any regulated community, establishing a relationship with regulators is imperative so as to ensure there is a level of trust, or more likely, what to expect with each phase or step of the program. As leadership changes, so do priorities and ways of implementing the various programmatic aspects, particularly with such a new program. As a result, the regulated community has found itself regularly investing effort in establishing a relationship and trust with the ISCD program leadership, only to have to repeat those efforts a year or two later.

Assuming he is executing the responsibilities of his position properly, the longer Wulf stays in the Director position, the better for the program, ISCD staff, and the regulated community. In adding Deputy Director Breor to the leadership team, DHS IP has further solidified the ISCD program and will send a clear message to all stakeholders that the Department is committed to the success of the program.

Increase the Utility and Ease of Use of the Security Plan

In terms of program execution, one of the more burdensome aspects of the CFATS program is the Site Security Plan (SSP). In fact, the Department originally estimated that the average SSP preparer would spend about 250 hours in developing and submitting an SSP via the CFATS program's on-line portal, the Chemical Security Assessment Tool (CSAT).[2] The CSAT SSP survey questions contributed to an end product that more closely resembles a checklist and inventory of chemicals, security measures, and other facility attributes, rather than a true operational plan. In practice, the CFATS SSP is purely a compliance tool and when not being reviewed or updated, the SSP likely sits on the shelf. So for those 250 hours of work in developing and submitting the plan, facility owners and operators do not regularly use the SSP—hardly a wise investment across an industry facing increasingly shrinking margins. In addition, the SSPs themselves did not elicit the appropriate information required by the DHS plan reviewers, requiring significant back and forth between DHS and a regulated facility, contributing to a substantial backlog in plan review and approval.

Fortunately, there is a more practical option provided for under the CFATS authorizing language that DHS has recently embraced and should enable a more efficient and effective security planning option. In developing an Alternative Security Plan (ASP), facilities may either leverage existing plans and repurpose them for regulatory compliance purposes, or utilize an industry format or template more familiar with corporate security types. As it so happens, many entities subject to the regulatory reach of the CFATS program also happen to be good corporate citizens and have adopted or ascribed to various voluntary security certification programs that establish industry security planning standards, such as the American Chemistry Council's Responsible Care Program and the Society of Chemical Manufacturers and Affiliates (SOCMA) Chem-Stewards Program. It is in allowing facilities to adopt these ASPs that ISCD may realize its greatest progress in moving through the SSP backlog, establishing a common baseline for security planning that is easy to both review and use. ISCD should further encourage the adoption of ASPs across industry, which would allow facilities to quickly adapt existing documents to satisfy CFATS requirements.

Finalize the Personnel Surety Program

The single greatest remaining policy challenge facing the Department related to the CFATS program is addressing the Personnel Surety requirements specified in the regulatory language. Under the "Personnel Surety" Risk-Based Performance Standard (RBPS), regulated facilities must put in place a series of measures to verify the identity of employees and unescorted visitors, check criminal history, validate legal authority to work, and look for terrorist ties.[3] The first three personnel surety elements are fairly standard and likely already a part of the on-boarding processes of most chemical companies. The fourth, however, poses a more significant challenge, as there is no central clearinghouse commercially available to check for terrorist ties.

(Continued on Page 15)

[2] http://www.gpo.gov/fdsys/pkg/FR-2012-12-17/pdf/2012-30313.pdf.

[3] 6 CFR 27.230 (a)(12).

Legal Insights

Is a 'Policy of Preemption' Replacing a 'Policy of Deterrence'?

The ability to subdue the enemy without battle is a reflection of the ultimate supreme strategy. The supreme is to attack enemies' strategies and plans, by thwarting them. (Chapter 3, Sun Tzu Art of War).

Based on the studies of Sun Tzu, one of the best forms of defense is considered to be a carefully judged and strategically timed attack on an enemy. Throughout history the preemptive use of force in the face of an imminent threat (preemption) has proven to be an effective strategy for self defense. International law recognizes a right of self-defense and the criterion for imminent threat, described as "instant, overwhelming, and leaving no choice of means, and no moment for deliberation."[1]

In 2002, the U.S. National Security Strategy began to redefine a policy of preemption. The implicit components of this redefinition represented a shift in how the U.S. views threats to national security and the homeland and how and when a specific threat should be neutralized. The administration argued that the classic doctrine of preemption should be expanded to deal with the emergent threats of transnational terrorist groups and others who seek to harm the United States. The rationale appeared to be two-fold: to deal with actors who cannot be reliably deterred, and to address the asymmetric threat posed by the use of ever more powerful weapons, especially WMDs.[2] In recent years the spectrum of threats has increased and now encompasses concerns such as cybercrime and attacks on critical infrastructure.

In the wake of the 2002 strategy (and its reaffirmation in 2006) a number of articles have been published, possibly none more thought provoking than the 2006 book *Preemption: A Knife That Cuts Both Ways* by Alan Dershowitz.[3] He notes: "The shift from responding to past events to preventing future harms is part of one of the most significant but unnoticed trends in the world today" and has prompted the question—is a policy of preemption the newest form of deterrence (the centerpiece of American foreign policy during the cold war)?[4] As Dershowitz argued "One of the great difficulties of evaluating the comparative advantages and disadvantages of deterrence versus preemption is that once we have taken preemptive action, it is almost never possible to know whether deterrence would have worked as well or better."[5]

Certainly the 2012 Defense Strategic Guidance of the Obama administration is no less focused on preemption than its predecessor when addressing the threats of transnational terrorists:

(Continued on Page 11)

[1] "Anticipatory Self-Defence Under International Law," *American University International Law Review*, Volume 19, Issue 1, Article 4 (2003).
[2] Michale E. O'Hanlon, Susan E. Rice, James B. Steinberg Policy Brief #113 (2002), The Brookings Institution..
[3] Alan M. Dershowitz. *Preemption: A Knife That Cuts Both Ways*. W.W. Norton & Company Inc. NY, NY ISBN 0-393-06012-8 (2006).
[4] In a speech given at the United States Academy at West Point, President Bush said, "those strategies [deterrence and containment] still apply. But new threats also require new thinking...to be ready for preemptive action when necessary to defend our liberty and to defend our lives." The White House, *President Bush delivers graduation speech at West Point*, (Washington, D.C.: Office of the Press Secretary, June 2002), available at: http://georgewbushwhitehouse.archives.gov/news/releases/2002/06/20020601-3.html.
[5] *Supra*, note 3.

(Continued from Page 10)

For the foreseeable future, the United States will continue to take an active approach to countering these threats by monitoring the activities of non-state threats worldwide, working with allies and partners to establish control over ungoverned territories, and directly striking the most dangerous groups and individuals when necessary.[6]

The most public example of such preemption is the United States use of unmanned aerial vehicles or 'drones' to address those threats. Supporters of preemptive strikes argue the United States should not have to wait to take action until it is on the verge of an actual attack and the United States has the right to self-defense. The White House argues that under Article 51 of the UN Charter, the United States has the right to self-defense when an imminent danger is present, and has applied this concept to carry out preemptive attacks.[7]

But what defines an imminent threat? The recently leaked and undated Department of Justice (DOJ) white paper reaffirms the U.S. government's authority to use preemptive lethal force; however, it is only limited to those who pose an imminent threat. The DOJ white paper also provides a broader meaning to "imminent" threat, defining it as the right of a state "to act in self-defense in circumstances where there is evidence of further imminent attacks by terrorist groups even if there is no specific evidence of where such an attack will take place or of the precise nature of the attack."[8] *The New York Times* recently reported that Central Intelligence Agency nominee John O. Brennan and President Obama have developed the administration's policies regarding the use of drones to conduct preemptive strikes against an imminent threat.[9] Although these policies on preemptive strikes are highly classified, White House spokesman Jay Carney expressed that "we conduct those strikes because they are necessary to mitigate ongoing actual threats, to stop plots, to prevent future attacks and, again, save American lives. These strikes are legal, they are ethical, and they are wise."[10]

The key premise that underpins a shift from deterrence to preemption is that many of the emergent and emerging threats are not deterrable, and as such, the argument for taking preemptive, preventive measures becomes even more compelling. In the case of transnational, non-state terrorists the argument has been debated and in the 'court of public opinion' held by the majority to be justifiable. But as a policy of preemption becomes more the norm, will that continue to be the case, especially when the choice of preemption versus deterrence seems more contentious?

In a companion article to this one Professor Jeremy Rabkin considers the emerging cybersecurity threat and offers his views on the possible use of strategies of preemption. Will this stand up to public scrutiny? Dershowitz suggested other threats that might see a future shift from deterrence to preemption—some of which will almost certainly raise strenuous objections (e.g. proactive crime prevention).

The question of whether or not a policy of preemption is replacing deterrence has already been affirmatively answered in the case of terrorist threats. It appears that some threats, like cyber, are heading in the same direction. The question is how far and how fast should the shift be going and who is asking the tough questions so that it remains an issue for thoughtful debate. The original test for the acceptable use of preemption was that of 'imminent threat'—perhaps now is the time to conduct an imminent review of this powerful yet somewhat troubling shift in policy. ❖

[6] Department of Defense, *Sustaining U.S. global leadership: Priorities for 21st Century defense*. (Washington, D.C.: White House, Secretary of Defense, January 2012), available at: http://www.defense.gov/news/defense_strategic_guidance.pdf, at 1.

[7] United Nations, Charter of the United Nations, Chapter VII, Article 51.

[8] Department of Justice, *Lawfulness of a lethal operation directed against a U.S. citizen who is a senior operational leader of al-Qa'ida or an associated force*, (Washington, D.C.: Department of Justice), available at: http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf, at 7. The DOJ white paper was leaked to MSNBC in February 2013.

[9] Michael D. Shear and Scott Shane, "Congress to see memo backing drone attacks on Americans," (*New York Times*, February 6, 2013), available at: http://www.nytimes.com/2013/02/07/us/politics/obama-orders-release-of-drone-memos-to-lawmakers.html?pagewanted=all&_r=0.

[10] Office of the White House Press Secretary, Press Briefing by Press Secretary Jay Carney, 2/5/13, (Washington, D.C.: Office of the White Press Secretary), available at: http://www.whitehouse.gov/the-press-office/2013/02/05/press-briefing-press-secretary-jay-carney-2513, par. 4.

(Continued from Page 3)

has taken place over time largely in the context of single agency initiatives or singularly focused "pilot projects." It is now time to put this capacity to use comprehensively and systematically across agencies and infrastructure sectors on a risk prioritized basis. Specifically, this integrated capacity should be utilized to conduct sophisticated analysis of complex infrastructure dependencies/interdependencies in the already defined high risk urban areas of the country, as well as in those regions prone to catastrophic natural disasters, within a 2-4 year timeline from start to finish. The results of this analysis should inform public-private preparedness planning, information sharing, training, and exercises in the high-risk regions of concern, and should be factored into FEMA grant guidance accordingly. These results should also feed real-time predictive analysis for emergent threats, as well as visualization and multi-level decision support for incidents in progress—particularly regarding the second and third order cascading effects of major disasters. As attested to by the initial lessons learned from the Super Storm Sandy response, critical infrastructure interdependencies and related impacts should never again represent an after-the-fact "strategic surprise."

- *Take Sector-Specific Plans to the Next Level.*

The Sector-Specific Plans (SSPs) under the National Infrastructure Protection Plan (NIPP) framework-have proven useful in characterizing the various critical sectors, identifying the public-private coordination elements of the various sector partnerships, framing a value proposition for sector collaboration, crystalizing sector-level goals and objectives, and cataloging various programs and activities geared toward the protection and resilience of sector infrastructure systems and assets. The next iteration of these very valuable partnering documents must include a detailed discussion of how the various programs and activities identified in the plans will be systematically utilized to understand and mitigate specific risks to the sector, along with specific timelines for doing so. Achieving this level of detail is critical to the path forward regarding performance measurement and resource allocation in the fiscally constrained world in which we are now operating.

- *Develop Focused Capabilities at the Regional and Local Levels.*

To put it succinctly, counterparts to the national level partnerships, information sharing mechanisms, risk assessment approaches, and risk mitigation programs championed in the NIPP and its SSPs must find their way to the regional and local levels if we are ever to achieve the strategic imperatives outlined above. Unfortunately, as budgets shrink and we move increasingly more distant from the 9-11 attacks, this is unlikely to occur in all the places where it needs to happen without a sustained Federal "push," in concert with key state and local government and private sector partners who have supported the NIPP framework over many years. The best way to jump start this activity (and, coincidentally, promote FEMA's "Whole Community" approach) is a partnership between DHS/NPPD FEMA, leveraging the in-place FEMA regional construct and DHS/NPPD Protective Security Advisor network. The first order of business of this partnership should be to spur public-private sector interaction in those regions and major municipalities where robust partnerships are not yet in place, beginning with focused joint risk assessment and planning activities as well as training and exercises.

- *Come to Terms with the Cyber Threat.*

The cyber threat represents a clear and present danger impacting all critical infrastructure sectors, particularly those we refer to as "lifeline infrastructures"—electricity, water, transportation, communications, health care, and emergency services. Although most of the critical infrastructure sectors have taken steps to understand and mitigate cyber risks internal to the sector (or sub-elements thereof), cross-sector cyber dependencies and interdependencies are not as well understood or mapped out. Getting a much better handle on such dependencies must become a focal point for joint public-private risk analysis, mitigation investment, and response/recovery planning moving forward. A more comprehensive understanding of the risks represented by this key emergent threat also warrants a great deal of public-private sector infrastructure community interaction in the form of joint training

(Continued on Page 13)

(Continued from 12)

and exercises. The importance of this interaction was noted in National Level Exercise 2012, which featured a complex and distributed set of cyber threats and attacks on government and privately-owned systems.

- *Re-energize and Empower the State and Local Government Stakeholder Base.*

In times of shrinking budgets and competing priorities, the Federal government must do all that it can to enable State and local government partners to achieve maximum effectiveness and efficiencies in executing their critical infrastructure protection and resilience responsibilities. Examples include highly fruitful programs such as the Automated Critical Asset Management System (ACAMS), a "user friendly" data and decision support system financed by the Federal government and used to facilitate infrastructure data warehousing, geospatial analysis, risk assessment, and contingency planning at the state and local levels, along with accompanying training and awareness programs. This "all-in-one" package has provided a huge boost to the critical infrastructure mission across all levels of government, facilitating engagement in this mission space down to the county level around the country. Another example is the capability achieved during the 2007/2008 hurricane seasons during which Federal assets were able to stream overhead imagery of impacts to critical infrastructure facilities within the storm damage footprint in real time to state, local, and private sector emergency operations centers via the Homeland Security Information Network (HSIN). Examples such as these demonstrate the power of Federal resources as key enablers supporting broader and deeper State, local, and private sector critical infrastructure mission execution.

- *Promote and Facilitate Private Sector Linkages to Fusion Centers and Emergency Operations Centers.*

Far too many high-risk regions and urban areas around the country still do not have formalized processes or mechanisms to integrate utilities, manufacturers, and small businesses into public sector information and intelligence sharing and emergency management activities. This is another area where significant Federal resources have been invested in pilot projects, information sharing tools, planning templates, best practices dissemination, etc. It's time to take stock of all these investments to date, focusing on the tools, best-practices, and templates that seem to make the most sense. We must then make a systematic, time-focused push for formal public-private sector information sharing integration in high-risk regions and localities where it matters the most and is currently lacking. This effort could be a primary initial focus of the DHS/NPPD and FEMA collaboration initiative discussed above. Public-private sector preparedness integration, with a focus on fusion center and emergency operations center linkages, also should figure prominently in DHS FEMA grant guidance looking forward.

Conclusion

We have come a long way in the critical infrastructure protection and resilience mission area since the darks days represented by the 9/11 attacks and Hurricane Katrina. Yet much remains to be done. In fact, given the dynamics of the global risk environment and the fiscal realities within which the "national team" must now operate, we stand to lose much of what we have attained if we don't stay focused and committed. The strategic imperatives outlined above are inherently achievable—even in an era of fiscal austerity—as long as we creatively and appropriately leverage the authorities, capacities, and resources of each member of the "national team." In the end, all this boils down to unity of effort, unity of purpose, and vision-driving programs (rather than vice versa) at all levels of government and the private sector to systematically identify and mitigate risk. If we get this right, the horrific cascading infrastructure failures and disruptions caused by Super Storm Sandy will have served as an important wake up call. If we fail, they will have served as a harbinger of events with potentially even more far-reaching consequences yet to come.❖

(Continued from Page 5)

ammonium nitrate as an explosive or as a fertilizer mixed with fuel to create Ammonium Nitrate/Fuel Oil (ANFO).[15] DHS's proposed regulations would implement registration activities and regulate "points of sale" by requiring ammonium nitrate facilities to verify that potential purchasers are properly registered with DHS.[16] Due to increased threats against our Nation's infrastructure, the second Obama Administration will probably push to finalize this proposed regulation.

Actions by the Executive Branch

The Cybersecurity Act of 2012, which failed to pass for the second time in the U.S. Senate in November 2012, would have directed DHS to set voluntary cybersecurity standards for companies that own and operate the Nation's critical infrastructure.[17] The proposed bill also would have implemented information-sharing requirements for cyber threats.[18] In the absence of new legislation, the Obama Administration has indicated that it will issue Executive Orders and Policy Directives to influence government entities and the private sector regarding critical infrastructure protection.[19] One draft proposed Executive Order released by the White House would institute voluntary cybersecurity standards similar to those in the Cybersecurity Act of 2012, but it would not include liability protections because such protections would require additional statutory authority. The draft Order directs DHS to coordinate the development of a Cybersecurity Framework which would use a flexible, sector-by-sector approach to reduce risk to critical infrastructure. Additionally, the draft Order directs DHS to identify critical infrastructure at greatest risk. It is likely that, in the absence of Congressional action, President Obama will issue a final cyber Executive Order.

In addition, the Obama Administration is expected to issue a proposed Critical Infrastructure Protection Policy Directive, which would likely rewrite Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7). [20] HSPD-7 established a national policy for prioritizing the protection of critical infrastructure and key resources (CIKR) from terrorist attacks.[21] The new Policy Directive will probably expand HSPD-7 to focus on improving the resilience of critical infrastructure, which DHS has defined as the "ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions."[22] A new Policy Directive will likely lead DHS to increase its focus on the protection of CIKR, the resilience of critical infrastructure against terrorist threats, and cybersecurity. Additionally, a new Policy Directive would impact the existing National Infrastructure Protection Plan (NIPP), which provides a unifying plan for protecting CIKR.[23] The NIPP was drafted in accordance with the HSPD-7 requirements to identify, prioritize, and coordinate the protection of CIKR from terrorist attacks.[24] If the Administration issues a new Policy Directive, DHS would likely expand the NIPP's current focus on protection to emphasize the resilience of CIKR in the event of a terrorist attack or natural disaster.

(Continued on Page 17)

[15] *Id.*

[16] *Id.*

[17] S. 2105, 112th Cong. (2012).

[18] *Id.*

[19] This article was submitted before the release of President Obama's executive order "Improving Critical Infrastructure Cybersecurity," on February 12, 2013.

[20] Homeland Security Presidential Directive-7 (Dec. 17, 2003).

[21] *Id.*

[22] DEP'T OF HOMELAND SEC., *Risk Steering Committee: DHS Risk Lexicon* 23 (Sept. 2008), http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf.

[23] DEP'T OF HOMELAND SEC., *National Infrastructure Protection Plan: Partnering To Enhance Protection And Resiliency* (2009), http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[24] Homeland Security Presidential Directive-7 (Dec.17, 2003).

(Continued from Page 9)

DHS, via the TSA Terrorist Screening Database (TSDB), however, does have a mechanism for checking those relationships, but no simple process in place to make it available to chemical facilities. TSA's Transportation Worker Identification Credential (TWIC) program, by its authorizing language, only extends to maritime facilities and vessels, and ISCD has been reluctant to adopt this program for CFATS purposes in the past. Moreover, ISCD does not necessarily want to be in the business of collecting information on U.S. citizens, particularly considering other components of DHS, like TWIC, already collect similar information.

In a series of fits and starts over the last several years, DHS has engaged industry to identify ways to facilitate checking against the TSDB. In the summer of 2012, DHS withdrew an Information Collection Request (ICR) to the Office of Management and Budget that was submitted in 2011. During congressional testimony later in the summer, DHS officials indicated that a new program would be announced in a matter of weeks and would likely include provisions permitting regulated facilities to utilize the TWIC program, which would expand the scope of the TWIC coverage. DHS, however, has not issued any additional details on the new approach as of early 2013.

Technical aspects of including the TWIC program aside, as well as the cost of implementing the program (which are not insignificant), TWIC may provide an elegant means of conducting a security assessment on personnel while "offshoring the risk" of collecting and processing employee information. The TWIC infrastructure is already in place to collect, process, and adjudicate decisions. By expanding the scope of the program and designating TWIC an acceptable form of screening, ISCD would effectively leverage economies of scale within DHS, in line with the Secretary's Efficiency Review Initiative.

Implementing the Ammonium Nitrate Program

Lastly, and not strictly a CFATS program issue (but under the umbrella and purview of ISCD) DHS was tapped by Congress in late 2007 with developing a program to regulate the purchase and distribution of Ammonium Nitrate (AN), the fertilizer that when added to fuel oil combines to make an explosive known as "ANFO." Timothy McVeigh notoriously used ANFO in the bombing of the Murrah Federal Building in Oklahoma City in 1995. DHS subsequently issued an Advanced Notice for Proposed Rulemaking for the AN Security Program in 2008, and almost three years later in 2011 issued a Notice of Proposed Rulemaking, detailing a conceptual regulatory program and soliciting comments on the program. DHS then held a series of public meetings, presumably to gather further information on ways to effectively and efficiently implement the AN security program. Since the early winter of 2011, however, the public record related to the AN security program is almost entirely silent as to the status of the program. Even Congress seems to have lost interest, holding no focused hearings on the DHS program. The House Homeland Security Committee did hold a closed hearing in August of 2012 reviewing the role of AN in improvised explosive devices. Although invited, DHS NPPD did not send a witness to participate in the hearing.

Regarding CFATS, DHS NPPD leadership long ago designated ISCD as the DHS office responsible for implementing the AN security program, leveraging the CFATS regulatory infrastructure to the extent possible. By any measure, this arrangement has not yielded the desired result (assuming DHS did in fact intend to proceed with the program), and by the milestones indicated in the legislative text that initially authorized it, DHS is approximately five years behind schedule. Recognizing the delay, DHS IP, under the leadership of Assistant Secretary Caitlin Durkovich, recently brought a seasoned chemical sector expert from elsewhere in IP into ISCD to take a leading role in the continued effort to stand up the AN security program. Under dedicated leadership, this long languishing program might finally see implementation and work to mitigate an identified risk.

Conclusion

Although these items are by no means an exhaustive list of policy related priorities Secretary Napolitano and DHS should

(Continued on Page 16)

(Continued from Page 15)

consider related to CFATS, they are the "big ticket" items that will lead to improved relations with both the regulated community and legislators. Some are clearly easier than others, but all are achievable and obtainable—and where further delays are identified, communicating and closely coordinating with interested stakeholders will engender significant good will. ❖

*Christopher C. Krebs, a graduate of the George Mason University School of Law, is a Principal with Obsidian Analysis, Inc. and previously served as Senior Policy Advisor to the DHS Assistant Secretary for Infrastructure Protection.

The Center for Infrastructure Protection and Homeland Security Presents:
Fatigue Risk Management in Aviation Operations

The Symposium will equip attendees with the knowledge and approaches necessary to effectivelty fight fatigue in the operational setting. The human physiology of fatigue and the hazards it represents in the workplace will be explored, along with the effective methods and tools to conduct fatigue risk management, mitigate fatigue's negative effects and enhanced public safety.

The one day session will be held May 1, 2013.

For more information on registration and agenda click here.

(Continued from Page 14)

Conclusion

While immigration will be a major homeland security focus during President Obama's second term, DHS will certainly make refinements to critical infrastructure protection over the next four years. In particular, as cybersecurity threats against U.S. industries continue to increase, the White House will push to strengthen cybersecurity standards for critical infrastructure. Other areas of focus for the Executive branch are likely to include the revision of CFATS and implementation of an ammonium nitrate regulatory program to address the increased threats against our Nation's infrastructure. ❖

Registration Now OPEN!

THE 2013 CRITICAL INFRASTRUCTURE SYMPOSIUM

"Advancing Full Spectrum Resilience"
April 15-16 • Thayer Hotel, West Point, New York

Hosted By: The Infrastructure Security Partnership, Society of American Military Engineers, the U.S. Army Corps of Engineers Engineer Research and Development Center, and the U.S. Military Academy at West Point

CELEBRATING 10 YEARS!
THE INFRASTRUCTURE SECURITY PARTNERSHIP

Please Click Here for Additional Information.

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