Ten Years After 9/11: Challenges for the Decade to Come

Paul Stockton

One of the best ways to honor those who perished on 9/11 is to rededicate ourselves to finding, and fixing, the gaps in preparedness that still confront our nation. Over the past decade, the Department of Defense (DoD) has greatly improved its ability to support the federal departments and agencies that lead US preparedness against terrorism and natural hazards. Yet, significant challenges remain in our ability to provide such defense support to civil authorities. Still greater shortfalls are emerging in a little-known but vital realm of preparedness: civil support to defense.

This essay begins by examining two gaps in DoD support to civil authorities. The first is DoD support to the Federal Emergency Management Agency (FEMA) for catastrophes more severe than Hurricane Katrina. The second gap is that of defense support to the civilian law enforcement departments and agencies that lead the prevention of terrorism in the United States.

I will then flip the familiar construct of defense support to civil authorities upside down, and explore the crucial roles that civilian agencies – and the private sector – can play to support the Department of Defense. I will argue that DoD is increasingly dependent on domestic infrastructure beyond the department's control, and that this infrastructure may be at growing risk of attack. I will also argue that only through new forms of civil-military cooperation can DoD ensure its ability to execute its core missions, at home and abroad. I hope that the shortfalls highlighted below will become part of the research agenda for graduate students and faculty, and a focus for the community of practice in homeland defense and security that is one of the greatest achievements of the past decade.

DEFENSE SUPPORT TO CIVIL AUTHORITIES

Complex Catastrophes

The Department of Defense is well prepared to support the Department of Homeland Security (DHS), FEMA and other federal departments and agencies in responding to "normal disasters" – that is, hurricanes, wildfires, and other events of typical magnitude, that most often spur governors to request federal assistance or prompt the federal government to position resources in anticipation of need. Of course, there are opportunities to improve our preparedness for normal disasters. Thanks to the leadership of the state governors, we are making progress across a broad range of issues in defense support for disaster response, especially in strengthening unity of effort between state and federal military response forces.[1]

The National Level Exercise 2011 (NLE 11) highlighted the need to strengthen our preparedness for events worse than normal disasters – disasters even more severe than Hurricane Katrina. NLE 11 was based on a scenario that began with a magnitude 7.7 earthquake along the New Madrid fault. An earthquake of that magnitude occurred in 1812; a similar one could strike at any time. The destructive effects could be far greater than two centuries ago, however. The Mid-America Earthquake Center notes that if such an event were to take place today, "the consequences would be much more significant and damage would be much more severe in terms of injuries and fatalities, structural damage, and economic and social impacts."[2] Indeed, the resulting devastation could so exceed the damage in normal disasters that these extraordinary events should be classified separately as "complex catastrophes."

Complex catastrophes differ from normal disasters in two ways. First, the scale of destruction is vastly greater. Katrina resulted

in 8,800 casualties, primarily (though not exclusively) in Louisiana and Mississippi. An earthquake like the one described in NLE 11 could inflict up to ten times as many casualties across eight states and four multi-state FEMA regions.[3] Localities and states near the New Madrid fault have made remarkable progress in improving preparedness for such an event. Nevertheless, the magnitude of the destruction and need for life-saving capabilities would almost certainly prompt governors to ask FEMA for large-scale federal assistance – with FEMA, in turn, asking DoD for unprecedented levels of defense support. Responding to those requests in a timely manner could create complex challenges for the department in sourcing the requested capabilities, transporting them, and then providing for their reception, staging, onward movement, and integration in a severely disrupted environment.

Second, as NLE 11 demonstrated, complex catastrophes may create cascading, region-wide failures of critical infrastructure, starting with the disruption of the commercial electric power grid. A 7.7 New Madrid earthquake would produce vastly greater damage to the grid than occurred in Hurricane Katrina or any other disaster in US history.[4] The net effect of physical damage to high-voltage transformers and other hard-to-replace components could be lengthy power outages across numerous states, with the potential for post-quake rolling blackouts also occurring in Chicago, the Eastern United States, and elsewhere.[5]

This loss of power could create cascading effects on communications and other critical infrastructure. From a public safety perspective, the most immediate concern might be the impact on municipal water systems, which in Memphis and most other cities depend on commercial electric power to operate. The loss of power could jeopardize the availability of drinking water from those systems. Transportation infrastructure could be degraded as well; gas and diesel fuel pumps, for example, depend on electric power to function. While many hospitals and other facilities critical to disaster response efforts have backup diesel-powered generators, we anticipate few will have sufficient fuel on hand to offset power outage lasting weeks to months, and that companies responsible for resupplying them could face a radical mismatch between supply and demand.

DoD is working today with FEMA and the DHS National Protection and Programs Directorate (NPPD), as well as other federal departments and agencies, to assess the lessons learned from NLE 11 and better prepare for complex catastrophes. Doing so will require innovative thinking on how to strengthen our preparedness. Consensus will be easy to reach on key foundations of our drive for greater preparedness. For example, in both complex catastrophes and normal disasters, the Post-Katrina Emergency Reform Act of 2006 (and the leadership role it assigns to the administrator of FEMA) will continue to govern response authorities and supported/supporting relationships. Other challenges of preparing for complex catastrophes could prove more difficult, however, starting with the need for better analysis of how cascading infrastructure failure could both increase requests for federal assistance, and make that assistance much more difficult to provide.

Defense Support to Law Enforcement

The most critical shortfalls revealed by 9/11 were not in disaster response, but rather in terrorism prevention. Over the past decade, the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and other federal, state, local, and tribal law enforcement agencies have made great strides in strengthening US prevention capabilities.[6] The efforts of DoD and its partners abroad have also weakened al-Qaeda. As President Obama notes, "we have put al-Qaeda on the path to defeat."[7] The president also notes, however, that "we continue to face a significant terrorist threat from al-Qaeda, its affiliates, and its adherents."[8] This threat includes efforts by al-Qaeda to inspire individuals within the United States to conduct their own attacks, and to disseminate plans on how to construct improvised explosive devices (IED).[9]

Of course, the primary DoD contribution to preventing terrorism against the United

States has been (and will remain) our operations abroad to disrupt, dismantle, and ultimately defeat al-Qaeda and its affiliates. The department also takes very seriously its responsibilities for homeland defense, In addition, within the United States, DoD supports – within the constraints set by the Constitution and other US law – its lead federal partners in their law enforcement efforts when they request prevention-related assistance. Those requests may grow in the future. For example, if terrorists were to launch a campaign using IED in the United States, DoD has technical expertise from dealing with such threats abroad that – consistent with US law – could be used to help meet requests for assistance by the FBI, DHS and other law enforcement agencies that would lead domestic counter-IED efforts.

President Obama has taken decisive steps to integrate US government prevention efforts more effectively. The June 2011 *National Strategy for Counterterrorism* lays out the overarching goals, and the steps to achieve them, that the US government will follow.[10] Presidential Policy Directive 8 (PPD-8), National Preparedness, further specifies how the United States will organize to meet the challenges of terrorism and other key hazards at home. Among other features, PPD-8 provides for the creation of a national preparedness system that will include a series of integrated national planning frameworks, covering prevention, protection, mitigation, response, and recovery. The frameworks – including prevention – will be supported by an interagency operational plan that provides a detailed concept of operations; a description of critical tasks and responsibilities; detailed resource, personnel, and sourcing requirements; and specific provisions for the rapid integration of resources and personnel. PPD-8 also requires the DoD and other federal departments and agencies to develop department-level operational plans, as needed, to support the interagency operations plans.[11]

The nation has long needed a national prevention framework. Now, thanks to PPD-8, we will soon have one. PPD-8 sets out stringent deadlines for the development of a national preparedness goal and the supporting preparedness system. Building out the prevention framework and the follow-on detailed operational plan will also require innovative thinking and new approaches to strengthen collaboration, across the federal government and among federal, state, local, tribal, and private sector entities.[12]

CIVIL SUPPORT TO DEFENSE

The concept of defense support to civil authorities is widely understood. Less familiar but increasingly important are opportunities for civilian agencies and private sector support to defense. Civilian agency support to DoD was very much in evidence on September 11, 2001. Firefighters, emergency managers, and law enforcement personnel from Arlington, Virginia, and other surrounding communities saved many lives at the Pentagon. We will always be grateful for their heroism. Their support that day also foreshadowed a growing challenge in the post-9/11 era. DoD is becoming ever more dependent on capabilities provided by civilian agencies and the private sector. Yet, those same capabilities are at increasing risk to cyber attack and other threats. New forms of civil-military cooperation are essential to meet the novel challenges of this era.

The Defense Industrial Base

DoD has long depended on the private sector to help arm and equip the armed services. But in the post-9/11 era, something important has changed: the Defense Industrial Base (DIB) is under cyber attack every day. The July 2011 *Department of Defense Strategy for Operating in Cyberspace* notes

> Foreign cyberspace operations against US public and private sector systems are increasing in number and sophistication. DoD networks are probed millions of times every day, and successful penetrations have led to the loss of thousands of files from US networks and those of US allies and industry partners.[13]

It is the responsibility of the Department of Homeland Security to protect the nation's critical infrastructure, and DIB is one of the eighteen critical infrastructure sectors under the National Infrastructure Protection Plan. Given the DoD's particular dependence on

the DIB, the need for DoD and DHS to partner with this sector against the threats they face is especially crucial.

Accordingly, the two agencies are now working closely with the DIB to increase the protection of sensitive information. The DIB comprises the public and private organizations and corporations that support DoD through the provision of defense technologies, weapons systems, policy and strategy development, and personnel. To increase protection of DIB networks, DoD launched the Defense Industrial Base Cyber Security and Information Assurance (CS/IA) program in 2007. Building upon this program, DOD is working with DHS to pilot a public-private sector relationship intended to demonstrate the feasibility and benefits of voluntarily increasing the sharing of information about malicious or unauthorized cyber activity and protective cyber security measures.[14]

Still to be determined is whether and how the models of the DoD-DHS relationship with the DIB might be extended to other parts of the private sector on which DoD depends. The DoD *Cyber Strategy* lays out some key considerations in this regard. The *Strategy* notes that public-private "partnerships will necessarily require a balance between regulation and volunteerism, and they will be built on innovation, openness, and trust." In some cases, incentives or other measures may be necessary to promote private sector participation. Efforts must also extend beyond large corporations to small and medium-sized businesses to ensure participation and leverage innovation."[15] These efforts are only just underway, and will require intense dialogue and new thinking on the part of all of those in this growing realm of collaboration.

Fortunately, DHS and DoD have shared interests and a strong partnership in this area. Last year, Secretaries Gates and Napolitano signed a memorandum of agreement laying out areas of joint cooperation in cyber security, to ensure that scarce resources are applied to the highest priority areas and to avoid unnecessary duplication of effort.

Fort Hood and the "Insider Threat"

DoD has traditionally focused on threats outside the perimeter of our military bases. Our adversary now seeks to exploit that familiar emphasis, and inspire attacks from within. Anwar al Aulaqi of al-Qaeda in the Arabian Peninsula is actively recruiting US military personnel and other radicalized US citizens to conduct "lone actor" attacks on US military targets. The author of *Inspire*, an English language magazine, intends to encourage and facilitate terrorist attacks on the United States. Al Aulaqi has been exhorting US sympathizers to conduct attacks similar to that which occurred at Fort Hood in November 2009: "This is because killing 10 soldiers in America for example, is much more effective than killing 100 apostates in the Yemeni military."[16]

DoD is already taking a range of internal measures to counter this new strategy. For example, military facilities in the United States now benefit from "active shooter" training programs that will enable their force protection personnel to counter insider threats more effectively. The DoD *Final Recommendations of the Ft. Hood Follow-on Review* identify a score of additional measures being implemented at military facilities nationwide to prevent a recurrence of the tragedy that struck Ft. Hood.[17] Other initiatives recommended in the report, however, will require longer-term academic and policy research.[18]

The need for innovation is even greater in those areas where DoD must depend on civilian departments and agencies to help DoD counter insider threats. Because DoD is generally restricted from collecting and storing law enforcement information on US citizens, DoD must rely on civilian agencies that play an increasingly important role in the overall system that protects US military facilities. As part of the Ft. Hood review, then-Secretary Gates directed several actions to improve DoD collaboration with the FBI at the Joint Terrorism Task Forces.[19] These ongoing efforts will be particularly effective in the context of a new, consolidated DoD-FBI Memorandum of Understanding being developed, aimed at promoting systemic, standardized information-sharing mechanisms and clarifying coordination

procedures as well as investigative responsibilities between DoD and FBI. DoD will also rely on FBI, DHS and the other civilian law enforcement agencies with which the FBI and DHS are networked to provide data on other domestic threats to U.S military installations, including "lone actor" attackers. Further, DoD, as part of its force protection efforts, is working closely with state and local law enforcement to recognize the indicators of a "lone actor" threat and share suspicious activity reports to prevent another Fort Hood type of attack from occurring. As this novel threat evolves, so too must the mechanisms by which the FBI and other civilian law enforcement agencies will support DoD.

Mission Assurance

The cyber threat to the DIB is only part of a much larger challenge to DoD. Potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities, by targeting the critical civilian and defense supporting assets (within the United States and abroad) on which our forces depend. This challenge is not limited to man-made threats; DoD must also execute its mission-essential functions in the face of disruptions caused by naturally occurring hazards.[20]

Threats and hazards to DoD mission execution include incidents such as earthquakes, naturally occurring pandemics, solar weather events, and industrial accidents, as well as kinetic or virtual attacks by state or non-state actors. Threats can also emanate from insiders with ties to foreign counterintelligence organizations, homegrown terrorists, or individuals with a malicious agenda.

From a DoD perspective, this global convergence of unprecedented threats and hazards, and vulnerabilities and consequences, is a particularly problematic reality of the post-Cold War world. Successfully deploying and sustaining our military forces are increasingly a function of interdependent supply chains and privately owned infrastructure within the United States and abroad, including transportation networks, cyber systems, commercial corridors, communications pathways, and energy grids. This infrastructure largely falls outside DoD direct control. Adversary actions to destroy, disrupt, or manipulate this highly vulnerable homeland- and foreign-based infrastructure may be relatively easy to achieve and extremely tough to counter. Attacking such "soft," diffuse infrastructure systems could significantly affect our military forces globally – potentially blinding them, neutering their command and control, degrading their mobility, and isolating them from their principal sources of logistics support.

The Defense Critical Infrastructure Program (DCIP) under Mission Assurance seeks to improve execution of DoD assigned missions to make them more resilient. This is accomplished through the assessment of the supporting commercial infrastructure relied upon by key nodes during execution. By building resilience into the system and ensuring this support is well maintained, DoD aims to ensure it can "take a punch as well as deliver one."[21] It also provides the department the means to prioritize investments across all DoD components and assigned missions to the most critical issues faced by the department through the use of risk decision packages (RDP).[22]

The commercial power supply on which DoD depends exemplifies both the novel challenges we face and the great progress we are making with other federal agencies and the private sector. Today's commercial electric power grid has a great deal of resilience against the sort of disruptive events that have traditionally been factored into the grid's design. Yet, the grid will increasingly confront threats beyond that traditional design basis. This complex risk environment includes: disruptive or deliberate attacks, either physical or cyber in nature; severe natural hazards such as geomagnetic storms and natural disasters with cascading regional and national impacts (as in NLE 11); long supply chain lead times for key replacement electric power equipment; transition to automated control systems and other smart grid technologies without robust security; and more frequent interruptions in fuel supplies to electricity-generating plants. These risks are magnified by globalization, urbanization, and the highly interconnected nature of people, economies, information, and infrastructure systems.

The department is highly dependent on commercial power grids and energy sources. As the largest consumer of energy in the United States, DoD is dependent on commercial electricity sources outside its ownership and control for secure, uninterrupted power to support critical missions. In fact, approximately 99 percent of the electricity consumed by DoD facilities originates offsite, while approximately 85 percent of critical electricity infrastructure itself is commercially owned.

This situation only underscores the importance of our partnership with DHS and its work to protect the nation's critical infrastructure – a mission that serves not only the national defense but also the larger national purpose of sustaining our economic health and competitiveness.

DoD has traditionally assumed that the commercial grid will be subject only to infrequent, weather-related, and short-term disruptions, and that available backup power is sufficient to meet critical mission needs. As noted in the February 2008 *Report of the Defense Science Board Task Force on DoD Energy Strategy*, "In most cases, neither the grid nor on-base backup power provides sufficient reliability to ensure continuity of critical national priority functions and oversight of strategic missions in the face of a long term (several months) outage."[23] Similarly, a 2009 GAO Report on *Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DoD Critical Assets* stated that DoD mission-critical assets rely primarily on commercial electric power and are vulnerable to disruptions in electric power supplies.[24] Moreover, these vulnerabilities may cascade into other critical infrastructure that uses the grid – communications, water, transportation, and pipelines – that, in turn, is needed for the normal operation of the grid, as well as its quick recovery in emergency situations.

To remedy this situation, the Defense Science Board (DSB) Task Force recommended that DoD take a broad-based approach, including a focused analysis of critical functions and supporting assets, a more realistic assessment of electricity outage cause and duration, and an integrated approach to risk management that includes greater efficiency, renewable resources, distributed generation, and increased reliability. DoD Mission Assurance is designed to carry forward the DSB recommendations.

Yet, for a variety of reasons – technical, financial, regulatory, and legal – DoD has limited ability to manage electrical power demand and supply on its installations. As noted above, DHS is the lead agency for critical infrastructure protection by law and pursuant to Homeland Security Presidential Directive 7. The Department of Energy (DOE) is the lead agency on energy matters. And within DoD, energy and energy security roles and responsibilities are distributed and shared, with different entities managing security against physical, nuclear, and cyber threats; cost and regulatory compliance; and the response to natural disasters. And of course, production and delivery of electric power to most DoD installations are controlled by commercial entities that are regulated by state and local utility commissions. The resulting paradox: DoD is dependent on a commercial power system over which it does not – and never will – exercise control.

Although there are steps DoD can and should take on its own to improve resilience and continuity of operations, achieving more comprehensive electric grid security to ensure critical DoD missions is not something DoD can do alone. Meeting and securing the critical electric power needs of DoD in an interdependent and increasingly complex risk environment requires a broad scope of collaborative engagement between government and industry stakeholders whose roles and responsibilities in power grid security and resiliency are distributed and shared.

DoD is collaborating with DOE, DHS, the Federal Energy Regulatory Commission, and industry representatives, namely the North American Electric Reliability Corporation (NERC), in these matters. For example, DoD is planning to develop a combined kinetic and cyber threat-based scenario for the US electric power grid. This scenario could be tested by DOE and others on a regional scale throughout the country and could produce data to support the development of a new system "design basis" for building additional

resilience in the US electric power grid. The department is also working with the NERC on a case study of a military installation for analysis, paired up with the local utility provider, to determine what can be done in the short term to mitigate electric power vulnerabilities and risks. DoD will make the results of this analysis more broadly available to DHS, DOE, and the industry. These efforts will help DoD achieve greater energy grid security and resiliency and help mitigate the risks to critical DoD missions from commercial power outages.

DoD is making organizational changes and capability improvements that address electric power reliability and security issues and that enable better risk-informed decision-making and investments. In January 2011, DoD submitted a report to Congress describing on-going efforts to mitigate the risks posed to critical DoD missions by extended power outages resulting from failure of the commercial electricity supply or grid and related infrastructure.[25]

In the report, DoD identified risks to the infrastructure supporting its key missions and is working with affected mission owners to "buy down" risk to an acceptable level. When fully implemented, risk reduction courses of action are aimed at reducing these risks to an acceptable level for DoD. DoD is conducting a series of case studies to identify the policy and technical issues associated with mitigating long-term electric power outages on installations. DoD is also planning and conducting demonstrations on installations to create cyber-secure power systems with microgrids and other smart grid technologies to improve electric grid security. The Marine Corps Air Ground Combat Center at Twentynine Palms, California, is implementing energy efficiency and alternative energy initiatives to demonstrate how microgrids will serve as an important component of the smart grid.

DoD established the Energy Grid Security Executive Council (EGSEC) to oversee many of these initiatives. The EGSEC brings together experts and senior executives from across DoD and from DOE and DHS to focus on ensuring the security of the electric grid that serves DoD. The EGSEC focuses on DoD energy grid vulnerability issues, the risk to critical missions created by commercial power outages, and developing comprehensive mitigating solutions.

We must identify and acknowledge our vulnerabilities and make the right choices – in collaboration with our strategic "partners" – to buy down our collective risk to an acceptable and affordable level in an informed way across the department. Determining how best to do that will require a sustained analytic effort and a willingness to collaborate in new ways. Driving that process forward, in the realm of mission assurance and so many others, would be a wonderful way to honor those who perished on 9/11.

ABOUT THE AUTHOR

Paul N. Stockton *is the assistant secretary of defense for Homeland Defense and Americas' Security Affairs. In this position, he is responsible for the supervision of homeland defense activities, defense support of civil authorities, and Western Hemisphere security affairs for the Department of Defense. From 2002 – 2006, assistant secretary Stockton served as director or the Naval Postgraduate School's Center for Homeland Defense and Security.*

[1] "DOD, Governors Bridge Gaps in Disaster Response," *American Forces Press Service*, March 11, 2011, http://www.defense.gov/news/newsarticle.aspx?id=63128.

[2] Amr S. Elnashai, Lisa J. Cleveland, Theresa Jefferson, and John Harrald, *Impact of New Madrid Seismic Zone Earthquakes on the Central USA* (Urbana, IL: Mid-America Earthquake Center, October 2009), http://mae.cee.uiuc.edu/publications/2009/09-03.htm.

[3] Ibid.

[4] The North America Energy Reliability Corporation estimated that the quake would instantly de-energize approximately 750 transmission lines and 300 substations in the region, and cause "extensive damage" to approximately half of the 500kV substations and other critical elements of the grid in Tennessee and Arkansas. North American Electricity Reliability Corporation, *Electricity Sector Damage Assessment for National Level Exercise 2011* (March 2011).

[5] Ibid.

[6] The White House, Executive Office of the President, *National Strategy for Counterterrorism* (Washington, DC, June 2011), 1, 11-12.

[7] *National Strategy for Counterterrorism*, i.

[8] Ibid.

[9] "How to Make a Bomb in the Kitchen of Your Mom," *Inspire,* Summer 2010, 33.

[10] *National Strategy for Counterterrorism*, 11.

[11] The White House, Executive Office of the President, Presidential Policy Directive-8 (Washington, DC, March 2011), 1-2.

[12] A prime example of the need for innovation: what concept of operations should these partners utilize in an IED campaign, or in a series of Mumbai-style attacks in US cities? How can we ensure that prevention, protection, and response efforts will be conducted in an integrated, mutually supportive fashion during such campaigns, amidst the crushing media and political pressures that will emerge? In light of the roles in defense support to civil authorities that DoD may assume under the prevention framework and implementation plan, how should DoD be postured to respond to requests for prevention assistance quickly and effectively, consistent with the Constitution and other US law, and recognizing the competing priorities DoD will face in a difficult fiscal environment? Answering these questions will require a strong analytic effort that leverages the expertise and perspectives of all the participants in the preparedness system that PPD-8 requires.

[13] US Department of Defense, *Strategy for Operating in Cyberspace* (Washington, DC, July 2011), 3.

[14] Ibid., 8.

[15] Ibid., 9.

[16] "Inspire Responses," *Inspire,* Spring 2011, 11.

[17] U. Department of Defense, Office of the Secretary of Defense, *Final Recommendations of the Ft. Hood Follow-on Review* (Washington, DC, August 2010), 10.

[18] For example, the Secretary of Defense issued interim guidance on indicators of violent behavior that will be modified with the completion of three studies. First is a Defense Science Board study projected for completion in early 2012. This study will be followed by two medical studies (a retrospective study and a prospective study) on DoD personnel. DoD will, as appropriate, incorporate the lessons of the studies into policies and programs upon study completion.

[19] *Ft. Hood Follow-on Review*, 10.

[20] US Department of Defense, *Mission Assurance Strategy*, draft, 1.

[21] Joseph Straw, "How to Take a Punch," *Security Management* (May 2011).

[22] RDP are risk management tools developed by the various asset owners and coordinated with the Combatant Commanders who rely upon these critical nodes to define the risk in terms of the existing threats and hazards, vulnerabilities of the existing system, and the consequence of loss if this node's support was interrupted. Asset owners then provide various courses of action (COA) to reduce this generated risk score to an acceptable level for the combatant commander. Once completed, these COA are prioritized so that the department knows exactly where to spend its limited resources most effectively.

[23] Defense Science Board, *Report of the Defense Science Board Task Force on DoD Energy Strategy: "More Fight, Less Fuel"* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2008),

[24] GAO Report 10-147, *"Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DoD Critical Assets"* (Washington, DC: October 2009).

[25] National Defense Authorization Act for Fiscal Year 2009, "Mitigation of Power Outage Risks for the Department of Defense Facilities and Activities" (Washington, DC: January 2011).