Testimony of the Honorable Paul Stockton
Assistant Secretary of Defense
Homeland Defense and Americas' Security Affairs
Department of Defense

Before the Subcommittee on Energy and Power
The Committee on Energy and Commerce
United States House of Representatives
May 31, 2011

Mr. Chairman and Members of the Committee:

I would like to begin by thanking you for the opportunity to testify today and for your interest in the security of the commercial electric power grid. I appreciate the vital role of Congress in the realm of energy security. Your leadership and leadership is critically important.

Also, I would like to thank two highly-valued and essential interagency partners: the Office of Electricity Delivery and Energy Reliability at the Department of Energy under Assistant Secretary Pat Hoffman; and the Office of Infrastructure Protection at the Department of Homeland Security under Assistant Secretary Todd Keil.

On this issue of great importance to the security of our nation, the Department of Defense is largely in a supporting role. The Department of Energy, the lead agency on energy matters, and the Department of Homeland Security, the lead agency for Critical Infrastructure Protection are in the lead. However, the Department of Defense is a significant stakeholder, and the Department's ability to perform its national security functions is largely dependent upon the reliability and resilience of the commercial electric power grid.

Department of Defense Reliance and Vulnerabilities

The Department of Defense relies on commercial electric power for nearly 99% of its power needs at military installations. Worldwide force deployment, support and sustainment, including that in Iraq and Afghanistan, are heavily dependent on commercial electrical infrastructure and associated supply chains. Since the events of September 11, 2001, many Department of Defense installations have changed and expanded their roles to include current operations "reach back"

in direct support of warfighting missions. A number of installations also serve as bases of operations to support Federal emergency relief and recovery efforts. Extended commercial power disruptions at these military installations could adversely affect power projection and homeland defense mission capability. In some cases, even short-term outages on installations can impact Department of Defense mission assurance.

The Department of Defense has limited back-up power. On-site back-up diesel generators are often used to support installation and facility continuity during short-term outages, but these generators are typically not designed to operate for extended periods. The average diesel generator and on-site fuel reserves are designed to sustain basic installation functions and critical missions for 3-7 days using fuel stored on-site. During small-scale power outages, military installations are able to manage fuel resupply through existing contingency plans – although most fuel pumping assets rely on electric power and will not operate during a power outage. However, the Department is just as reliant on diesel fuel generators as the civilian sector is and will face similar reliability and fuel issues.

In the case of a large-scale power disruption, fuel resupply on military installations could be significantly compromised due to competing demand with local and regional government and population requirements for fuel distribution. While there are existing legal authorities such as the Defense Production Act that would ensure that in such extraordinary circumstances military needs would be met large-scale power disruptions that effect military installations and our Defense Industrial Base facilities could have potentially catastrophic mission impacts that we do not yet fully understand.

Nature of the Threat

The commercial electric power grid is increasingly threatened by a convergence of challenges that could lead to electric power disruptions that have the potential to challenge our nation's defense capabilities. This complex risk environment includes: disruptive or deliberate attacks, either physical and cyber in nature; natural hazards such as geomagnetic storms, and natural disasters with cascading regional and national impacts; long supply chain lead times for key replacement electric power equipment; increases in energy demand surpassing production and distribution; aging infrastructure; and transition to automated control systems and other smart grid technologies.

Mr. Chairman, I am going to refrain from speaking in any more detail on the nature of our adversarial threats, but please allow me to share a couple of examples related to the impacts natural disasters can have on the Department of Defense. The threat posed by space weather events is a serious challenge to our national security. A strong electromagnetic pulse from a solar storm can fuse the copper wires of high-voltage transformers, damaging them beyond repair. The National Academies of Science reports that if solar storms occurred today comparable to those that took place in the United States in 1921, more than 350 transformers could suffer permanent damage, leaving as many as 130 million people without power. While it is difficult to project the probability of such events, extended power outages at Department of Defense installations would significantly affect the Department of Defense's execution of key missions, both here in the United States and overseas. Projection of military force overseas and homeland defense mission capability is heavily dependent on commercial critical infrastructure and supply chains, which all rely on the electric grid for power. Large-scale power disruptions could also have significant impact on our defense support of civil authorities' mission. There would be substantial calls for National Guard support to basic public safety functions and human needs. This would be the federal government, and Department of Defense's priority. One particular area of concern is our ability to receive and stage our consequence management forces due to the loss of power and damage to the communication and transportations sectors.

This year's National Level Exercise was based on a major earthquake scenario that occurs along the New Madrid Seismic Zone. The initial 7.7 magnitude earthquake and subsequent 6.0 magnitude earthquake would cause extensive damage to the electric grid across several States. The first quake would instantly de-energize approximately 750 transmission lines and 300 substations. This would likely affect 100-150 million people, with the Northeast, Southwest and Midwest experiencing most of the outages. Many areas of the Eastern Interconnection would have down times of at least 14 hours to 5 days. Areas suffering physical damage could have much longer down times ranging into weeks and months depending on damage to long lead-time items like transformers and towers. According to an electricity sector damage assessment by the North American Electric Reliability Corporation approximately half the 500kV substations in Tennessee would be considered "Extensively Damaged". For Arkansas, at least half the 500kV and a significant portion of the 230kV substations would be "Extensively Damaged". The New Madrid quake would cause one of the largest electrical pathways to be interrupted, and likely cause complete destruction of multiple substations.

We simply don't understand the potentially cascading effect that could result from a large-scale, long-term loss of electric power. The bottom line is that we are not where we need to be in really understanding how all of these components are interconnected.

Interagency and Industry Collaboration

The Department of Defense fully recognizes the strategic importance of mitigating the growing risks to the commercial electric power grid, and therefore, the Department is taking affirmative steps internally and externally. Senior leaders are re-focusing some of the Department's energy security efforts.

Although there are steps the Department can and should take on its own to improve resilience and continuity of operations, achieving more comprehensive electric grid security to ensure critical Department of Defense missions is not something the Department of Defense can do acting alone. Meeting and securing the Department of Defense's critical electric power needs 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. While there are maintenance and on-site power surety efforts that need some new focus, for the Department of Defense to succeed in this challenge, leadership and support from industry representatives and interagency partners at various levels of government are imperative.

The Department of Defense is collaborating with the Department of Energy, the Department of Homeland Security, the Federal Energy Regulatory Commission and industry representatives, namely the North American Electric Reliability Corporation, in these matters. For example, we are planning to develop a combined kinetic and cyber threat-based scenario for the U.S. electric power grid that could be applied on a regional scale throughout the country and be used to support the development of a new system "design basis" for building additional resilience in the U.S. electric power grid. We are also working with the North American Electric Reliability Corporation on planning 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. The Department is also participating in exercises such as the recent National Level Exercise-11 exercise and upcoming Departments of Homeland Security, Energy and Defense sponsored Secure Grid 2011 and the North American Electric Reliability Corporation's GridEx 2011.

These partnerships will help the Department of Defense achieve greater energy grid security and resiliency and help mitigate the risks to critical Department of Defense installations and facilities of commercial power outages.

Department of Defense Efforts Underway

The Department of Defense 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.

This year the Department of Defense submitted a report to Congress under Section 335 of the 2009 National Defense Authorization Act. Section 335 requires the Department to submit an annual report to Congress on efforts to mitigate the risks posed to Department of Defense mission critical installations, facilities, and activities by extended power outages resulting from failure of the commercial electricity supply or grid and related infrastructure. Congress enacted Section 335 of the National Defense Authorization Act in response to the publication of a 2008 Report by the Defense Science Board on the Department of Defense Energy Strategy, titled "More Fight, Less Fuel." The report found that "critical national security and homeland defense missions are at an unacceptably high risk of extended outage from failure of the [commercial electrical power] grid" upon which Department of Defense overwhelmingly relies for its electrical power supplies.[1]

I would like to highlight several Department of Defense initiative that serve to foster improvements in electric grid security.

Energy Grid Security Executive Council

The 2008 Defense Science Board Report recommended that the Department of Defense establish an interagency oversight group on commercial electric grid issues because within the Department of Defense, there is no central authority on energy security matters. Energy security roles and responsibilities are widely distributed, with different entities managing security against physical, nuclear, and cyber threats, cost and regulatory compliance, and the response to natural disasters. More than a year ago, the Department of Defense established the Energy Grid Security Executive Council. The Energy Grid Security Executive Council brings

[1] Report of the Defense Science Board Task Force on Department of Defense Energy Strategy, *"More Fight – Less Fuel"*, February 2008

together experts and senior executives from across the Department of Defense and the Departments of Energy and Homeland Security to focus on ensuring the security of the electric grid that serves the Department of Defense. The Energy Grid Security Executive Council focuses on the Department's energy grid vulnerability issues, the risk to critical missions created by commercial power outages, and developing comprehensive mitigating solutions.

Further, the Energy Grid Security Executive Council helps identify gaps and deficiencies and recommended approaches to secure access to adequate and reliable energy sources necessary to ensure continuity of critical defense missions in the event of extended failure of commercial energy infrastructure. The Energy Grid Security Executive Council makes use of existing Department of Defense legal and budgetary authorities and seeks to achieve greater electric grid security through development, coordination and oversight of policies, strategies, plans and initiatives.

Homeland Defense Energy Security Case Studies

I initiated a series of regional Energy Security Case Studies in January 2010 to address the policy and technical issues necessary to mitigate the risks of long-term electric power outages to clusters of Department of Defense and Defense Industrial Base sites. The Energy Grid Security Executive Council provides oversight of this effort. The case studies are consistent with requirements under Section 335 of the 2009 National Defense Authorization Act and a 2008 Defense Science Board Report recommendation that the Department of Defense take actions to "island" installations from the commercial electric power grid. [2]

The case studies are an attempt to analyze the impact of an extended power outage and the potential range of feasible Department of Defense and interagency solutions, much like an analysis of alternatives. The studies are intended to help set the stage for defining the size and scope of the issue and to help facilitate the requirements process. They will help define where Department of Defense's prudent investments should end and where commercial and civil authorities, responsibilities and investments should begin. The case studies approach is designed to provide greater electric power security to a region by separating key elements of generation and distribution infrastructure from the grid as an independent operating unit or "island". The island would be capable of generating

[2] Report of the Defense Science Board Task Force on Department of Defense Energy Strategy, "More Fight – Less Fuel", February 2008

and distributing electric power if the grid (outside the region) is disrupted for either short or extended periods of time.

The first of three Case Studies was initiated in May 2010 in the Norfolk, Virginia region. The Navy's Dahlgren Mission Assurance Division completed the assessment phase (the first of three phases) for the Norfolk case study on May 13th. The Norfolk Region Assessment Phase recommended two risk mitigation approaches for operating electrical systems in support of the identified critical Department of Defense missions for extended electrical power outages.

The two mitigation approaches identified include working with the local utility to establish a load management schematic to ensure both critical Department of Defense and non-Department of Defense assets (such as life safety and supporting infrastructure) have sustained stable power in the event the load exceeds available generation. The study also recommends a second approach that separates the mission critical functions, those identified during the mission analysis, from the commercial grid and establishes separate microgrids using an integrated network of back-up generators on the installation. This enable Department of Defense to manage the load and generation within the microgrids, ensure constant and stable power to critical Department of Defense missions and reduce the overall load in the region providing the utility provider with additional flexibility stabilizing the grid and providing power to the community. Pursuing both mitigation approaches optimizes management of electric power for critical Department of Defense missions, supporting infrastructure and broader community needs. There are several potential options for finding a balance between commercially-generated and government-generated power on the installations that will be explored.

The Mission Assurance Division recently initiated phase II (solutions refinement) to refine the recommended mitigation approaches and develop a technically relevant and feasible mitigation plan. A second case study is underway at Vandenberg Air Force Base in California, with a set of preliminary findings and recommendations due in July 2011. A third case study is in the initial planning stages and will include a cluster of Defense Industrial Base facilities in Texas.

All case studies are pursuing the goal of mitigating the risks to Department of Defense missions caused by long-term electric power outages. The end state is a comprehensive, adaptable, and repeatable methodology to identify high-order commercial electric power-related risks on a regional basis throughout the United States and develop and implement appropriate mitigation solutions.

Marine Corps Air Ground Combat Center Base Twentynine Palms

At Twenty Nine Palms, a Marine base in the Mojave Desert, we are demonstrating new micro-grid technology—a system of self-generated electricity and intelligent controls that can be operated independently if the commercial grid goes down. Micro-grids improve energy efficiency, make it easier to incorporate solar and wind power, and ensure power can be directed to facilities that need it most. Most importantly, they reduce the vulnerability of our power supplies to disruption.

The remote base in the Mojave Desert serves a population of more than 27,000 military and civilian personnel who facilitate large scale training and exercises. The austere conditions, limited infrastructure and continuity of operations place a heavy demand on the base's electrical infrastructure. The California base sustains its mission with over 10MW of power generated on site by a 2MW solar photovoltaic farm, 1MW of solar photovoltaic shading, a 0.5MW fuel cell and a 7.2 MW Cogeneration plant. The base is tying together its disparate electrical infrastructure in an optimal way while serving as a test bed for new technologies through various Department of Defense initiatives including the Environmental Security Technology Certification Program. The centerpiece of the facilities electrical infrastructure integration is being implemented to demonstrate how microgrids will serve as an important component of the Smart Grid.

Key features of the Twentynine Palms microgrid include centralized supervisory control, distributed metering and a secure wireless network to create a self-contained system capable of unplugging from the utility grid. The microgrid is a smart power distribution system that both manages and optimizes the flow of electricity around the base. The microgrid is particularly adept at dealing with the variability of intermittent renewable energy generation, combining it with energy storage and ensuring power quality and reliability. Additionally, the microgrid addresses the demand side of the energy system and sheds loads when needed.

Demonstration projects like the Twentynine Palms microgrid aim to increase energy security on Department of Defense installations, while reducing energy consumption and managing electricity usage more effectively. Many military installations, like Twentynine Palms, will serve as examples of how communities and campuses can develop their own microgrids. Remote communities in particular will look to facilities like Twentynine Palms for insights and best practices.

Energy Surety Microgrid

The Department of Energy currently funds an effort at Sandia National Laboratory to investigate new approaches for secure and robust power sources near critical loads and ways to better manage existing power generation and loads to improve the reliability and security of electric power at military installations. The Sandia approach, called the Energy Surety Microgrid, is an alternate energy delivery methodology developed to ensure that the reliability of the electric infrastructure at a given military facility will fully satisfy critical mission needs. The Sandia Energy Surety Microgrid methodology identifies buildings and operations at military facilities that are mission critical, and creates a secure and reliable power system to support these missions for the durations required.

Demonstration of Electric Grid Security Architecture

Building on the Sandia Energy Surety Microgrid project, U.S. Pacific Command and U.S. Northern Command proposed a comprehensive microgrid candidate demonstration of a cyber-secure electric grid security architecture in partnership with the Departments of Energy and Homeland Security. The demonstration plans to include cyber-secure smart microgrids with demand side management and integration of renewable energy and energy storage on military installations for improved mission assurance during prolonged outages of commercial power. The demonstration would also include integration of cyber-secure industrial control systems; application of Smart Grid technologies; distributed and variable renewable generation and energy storage; and redundant, distributed back-up power generation.

The application of cyber-secure smart microgrids on military installations would not replace commercial power as a primary source, but would enable reliable, secure, and sustainable backup power for critical missions at the installation level. The results of the demonstration would help inform infrastructure investment decisions needed to reduce the risk of extended electric power outages to military installations and potentially, the surrounding civilian communities.

Conclusion

Mr. Chairman, I would like to close by emphasizing that continued leadership and support from Congress, our lead Federal agencies and industry is

imperative for the Department of Defense to succeed in achieving greater electric grid security for Department of Defense installations and critical missions.

I would like thank you again for the opportunity to testify today and for your interest in the security of the commercial electric power grid.

With the assistance of its partners, the Department of Defense will continue actively test energy security and resiliency solutions, and to implement short, medium, and long-term plans and mitigation actions necessary to secure critical missions.

Thank you, and I very much look forward to your questions.