Off the Grid: Facilitating the Acquisition of Microgrids for Military Installations to Achieve Energy Security and Sustainability

Thomas Joseph Alford*

The attack took less than twenty minutes. From a berm overlooking the perimeter fence of Pacific Gas and Electric ("PG&E")'s Metcalf electrical substation, a group of saboteurs opened fire upon the facility.[1] One surveillance camera pointed along the perimeter recorded a streak of light, followed closely by the muzzle flashes of rifles.[2] The station's motion alarm failed to sound until nearly halfway through the barrage, when one of the sniper's bullets ricocheted with a bright spark off the fence.[3]

Using the cover of darkness and an arsenal of Kalashnikov rifles, the attackers were all targeting the same thing: The large, oil-filled cooling drums that sit atop the substation's several electric transformers.[4] Peppered with 7.62x39mm bullet holes, the tanks eventually leaked over 52,000 gallons of cooling oil, which, very quickly, led to the transformers overheating, and then shutting down altogether.[5] In order to avoid a complete blackout of Silicon Valley, the California electric-grid officials responding to the attack scrambled to reroute power around the transmission substation,[6] and quickly requested other power plants in the area to pick up the slack.[7]

After nineteen minutes of sustained and precise shooting, the attackers disappeared into the night.[8] The more than 100 shell casings later found near the scene were completely fingerprint-free.[9] Of the boot prints left behind, not one could be identified. And, no getaway vehicle tracks were ever found.[10] Police did, however, find small piles of rocks from which the attackers were shooting that appeared to have been set up in advance in order to position the snipers for the most accurate shots.[11]

* *The author, Major Thomas J. Alford, is an officer in the United States Air Force and has been designated a Judge Advocate by The Judge Advocate General of the Air Force.* *This Article was submitted in partial satisfaction of the requirements for the degree of Master of Laws in Government Procurement and Environmental Law at The George Washington University School of Law. The views expressed in this Article are solely those of the author and do not reflect the official policy or position of The Judge Advocate General's Corps, the Department of the Air Force, the Department of Defense, or the United States Government. The author wishes to thank Dean Lee Paddock and Professor Donna Attanasio, who both provided valuable insight needed in completing this Article. He also wishes to thank his wife, Polina Alford, for her patience and love throughout the school year. Major Alford was also the recipient of the 2017 Jamie Grodsky Prize for Environmental Law Scholarship. The prize recognizes an original paper by a George Washington University Law student in the environmental field as judged by a panel.*

1. Rebecca Smith, *Assault on California Power Station Raises Alarm on Potential for Terrorism*, Wall St. J., Feb. 5, 2014 [hereinafter Smith, *Assault on California Power Station Raises Alarm on Potential for Terrorism*], http://www.wsj.com/articles/SB10001424052702304851104579359141941621778.
2. *Id.*
3. *Id.*
4. Alexis C. Madrigal, *Snipers Coordinated an Attack on the Power Grid, but Why?*, Atlantic, Feb. 5, 2014, http://www.theatlantic.com/technology/archive/2014/02/snipers-coordinated-an-attack-on-the-power-grid-but-why/283620/ ("Whoever executed the maneuver knew where to shoot the transformers.").
5. *Id.*; Smith, *Assault on California Power Station Raises Alarm on Potential for Terrorism*, *supra* note 1.
6. A transmission substation connects two or more power transmission lines and frequently contains two or more large transformers. Transformers raise electricity voltage so it can travel large distances on high-voltage lines. *See* U.S. Dep't of Agric. Rural Utils. Serv., RUS Bull. No. 1724E-300, Design Guide for Rural Substations 39 (2001), http://www.rd.usda.gov/files/UEP_Bulletin_1724E-300.pdf.
7. Smith, *Assault on California Power Station Raises Alarm on Potential for Terrorism*, *supra* note 1.
8. *Id.*
9. *Id.*
10. Richard A. Serrano & Evan Halper, *Sophisticated but Low-Tech Power Grid Attack Baffles Authorities*, L.A. Times, Feb. 11, 2014, http://www.latimes.com/nation/la-na-grid-attack-20140211-story.html.
11. Smith, *Assault on California Power Station Raises Alarm on Potential for Terrorism*, *supra* note 1.

It has now been over 3 years since the April 16, 2013 attack on PG&E's Metcalf Transmission Substation, located outside of San Jose, California, adjacent to U.S. Highway 101. To this day, no suspects have been apprehended, and no motive for the attack has been identified.[12] Although the military-style raid on the power substation successfully disabled seventeen giant transformers and six circuit breakers for 27 days, caused over $15 million in damages, and came close to knocking out all power in Silicon Valley,[13] the attack was barely covered by the national news media.[14] Yet, the sophisticated nature of the attack—the fact the attackers brought night-vision scopes for their weapons, used heavy wire cutters to sever fiber-optic telephone cables in a subterranean vault prior to the assault, and strategically chose a location near a major U.S. highway to escape—has officials concerned about future coordinated attacks on the Nation's power grid.[15] Thus, whether it was intended or not, the brief, but ferocious attack revealed how vulnerable and unprotected the U.S.'s power grid truly is.

Jon Wellinghoff, chairman of the Federal Energy Regulatory Commission ("FERC") at the time of the attack called it "the most significant incident of domestic terrorism involving the grid that has ever occurred."[16] He added that if a "surprisingly small" number of U.S. substations were incapacitated at one time, then it could lead to a power blackout of most of the U.S.[17] Other officials have voiced concern that too many "people in the electric industry have been distracted by cybersecurity threats," and that physical attacks, like the one carried out against the PG&E facility, represent a "big, if not bigger" threat.[18]

For those who were alive to witness the terrorist attacks on September 11, 2001, a coordinated attack on the U.S. by either terrorists or an adversarial nation state can no longer be dismissed as a mere farfetched Hollywood plot.[19] Where the September 11th terrorist attacks were carried out using hijacked Boeing 757 and 767s as missiles, an attack against the Nation's power grid could start with only the press of a button, the flip of a switch, or, like the attack against the PG&E facility, the squeeze of a few triggers. It has been said that the failure to prevent the terrorist attacks on September 11, 2001 was, in large part, due to a "failure of imagination" by the U.S. officials responsible for the Nation's defense.[20] But, with much of the U.S.'s defense infrastructure reliant upon an aging and largely unprotected civilian power grid,[21] it does not take a great deal of imagination to envision what kind of harm a determined enemy could inflict if it exploited such a vulnerability: Without power, computer screens across the Department of Defense ("DoD")'s installations would go blank. Fuel pumps would lock. Air traffic would be halted. Flights grounded.

As the institution ultimately responsible for protecting the Nation, the DoD can no longer rely upon the vulnerable commercial power grid for the lion's share of its energy needs.[22] The acquisition of a more reliable and resilient system, which would allow the DoD's critical assets to function in the event of a catastrophic failure of the commercial grid, is an absolute necessity for our Nation's defense.[23] Emerging

12. In October of 2015, however, DHS's Assistant Secretary for Infrastructure Protection, Caitlin Durkovich, stated that there were "indications" that the attack was carried out by a PG&E "insider." *See* Jose Pagliery, *Sniper Attack on California Power Grid May Have Been "an Insider," DHS Says*, CNN Money, Oct. 17, 2015, http://money.cnn.com/2015/10/16/technology/sniper-power-grid/.
13. *Id.*; Smith, *Assault on California Power Station Raises Alarm on Potential for Terrorism*, *supra* note 1.
14. Likely due, in part, to the attack's proximity to the April 15, 2013 Boston Marathon bombings.
15. Serrano & Halper, *supra* note 10 ("The perpetrators arrived shortly before 1 a.m. and were gone 52 minutes later. Apparently the first call to authorities came from a driver speeding by on U.S. 101 . . . 'Fireworks were coming from the substation,' [the driver] said.").
16. Smith, *Assault on California Power Station Raises Alarm on Potential for Terrorism*, *supra* note 1 ("This wasn't an incident where Billy-Bob and Joe decided, after a few brewskis, to come in and shoot up a substation," Mark Johnson, retired vice president of transmission for PG&E, told [a] utility security conference, "[t]his was an event that was well thought out, well planned and they targeted certain components."). Navy SEALS who toured the site with Mr. Wellinghoff not long after the attack were convinced that the attack was a professional job. *See* Madrigal, *supra* note 4, at 2. Officials within the Federal Bureau of Investigation ("FBI"), however, stated that the attack was likely not an act of terrorism since, among other reasons, "Terrorists want credit for their acts . . . .[and there's] been none here, no claims of responsibility." David R. Baker, *FBI: Attack on PG&E South Bay Substation Wasn't Terrorism*, S.F. Chron., Sept. 11, 2014, http://www.sfgate.com/business/article/FBI-Attack-on-PG-amp-E-substation-in-13-wasn-t-5746785.php.
17. Smith, *Assault on California Power Station Raises Alarm on Potential for Terrorism*, *supra* note 1; *see also* Strategic Plan *infra* note 19, at 7 ("[T]he interconnected nature of critical infrastructure can also result in unanticipated and cascading impacts from events across infrastructure sectors and geographical areas.").
18. Smith, *Assault on California Power Station Raises Alarm on Potential for Terrorism*, *supra* note 1.
19. *See e.g.*, Nat'l Prot. & Programs Directorate, U.S. Dep't Homeland Sec., Office of Infrastructure Protection Strategic Plan: 2012–2016, at 1 (2012) [hereinafter Strategic Plan], https://www.dhs.gov/sites/default/files/publications/IP-Strategic-Plan-FINAL-508.pdf (statement of Caitlin A. Durkovich, Assistant Secretary, Office of Infrastructure Protection) ("[E]vents of the 21st century have already shown that we live in a dynamic and global risk environment, defined by new and evolving threats and challenges to the Nation's infrastructure.").
20. *See* The 9/11 Comm'n Rep., Final Rep. of the Nat'l Comm'n on Terrorist Attacks Upon the U.S. 344 (2004), http://govinfo.library.unt.edu/911/report/911Report.pdf ("Imagination is not a gift usually associated with bureaucracies.").
21. Meagan Clark, *Aging U.S. Power Grid Blacks Out More Than Any Other Developed Nation*, Int'l Bus. Times, July 17, 2014, http://www.ibtimes.com/aging-us-power-grid-blacks-out-more-any-other-developed-nation-1631086; Michael Wu, *Congress Must Protect Military Energy Security*, Hill (June 30, 2014), http://thehill.com/blogs/congress-blog/homeland-security/210855-congress-must-protect-military-energy-security ("Our military installations rely on the civilian grid for 98[%] of their electricity requirements, but our grid is increasingly old, fragile, and threatened.").
22. Def. Sci. Bd., Report of the Defense Sciences Board Task Force on DOD Energy Strategy: "More Fight—Less Fuel" 18 (2008) [hereinafter Def. Sci. Bd., More Fight—Less Fuel], http://www.acq.osd.mil/dsb/reports/ADA477619.pdf ("About 85% of the energy infrastructure upon which DoD depends is commercially owned, and 99% of the electrical energy DoD installations consume originates outside the fence.").
23. Because of this clear and present threat to national security, this Article is intended to be a canary in the mine shaft. Though it is, by no means, the first to chirp. *See, e.g.*, Ashleigh Acevedo, *Enlisting Renewable Energy: The Military's Environmental Exceptionalism and a Renewable Energy Initiative in the Face of a National Security Threat*, 45 Tex. Envtl. L.J. 343 (2015); Sarah E. Light, *The Military-Environmental Complex*, 55 B.C. L. Rev. E. Supp. 879 (2014) (primarily concerned with the threat of climate change); Jeremy S. Scholtes, *On Point for the Nation: Army and Renewable Energy*, 34 Energy L.J. 55 (2013) (primarily concerned with the threat of climate change); Cameron E. Tommey, *Moving Military Energy "Behind the Fence": Renewable Energy Generation on U.S. Defense Lands*, 6 Wash. & Lee J. Energy Climate & Env't 592 (2015), http://scholarlycommons.law.wlu.edu/jece/vol6/iss2/8). These articles will be discussed in greater detail *infra*.

technologies—microgrids[24] and large scale battery storage—must be deployed as they continue to be developed, and the DoD must also continue its movement towards decentralized, on-site energy generation on its installations.[25]

Among federal agencies, the DoD is in a unique position to act as a model to tackle and, perhaps, even solve the energy security and sustainability issues facing the Nation.[26] The agency is allocated a large portion of the federal budget, it is responsible for managing significant tracts of unused but useful land, and it acts as a massive individual consumer of domestic energy.[27] The DoD is also known to be a catalyst for and a cultivator of technological innovation,[28] and it has already begun spearheading an effort to move the federal government writ large towards the use of more renewable energy sources. While the DoD has been making *ad hoc* progress towards energy security, there remains significant room for improvement. This Article will focus on the needed legal, regulatory, and practical reforms to facilitate that improvement.

Part I of this Article will explore the present threat environment, including the threat to the Nation's electricity infrastructure, as well as the risk of the DoD continuing to rely upon the commercial grid for its energy needs. The solution of going "off the grid" using microgrids and on-site renewable energy will also be discussed.

Part II examines the policy solutions already being applied in an attempt to address the DoD's energy security issues. This includes a discussion of the renewable energy mandates from both Congress and the President, and the renewable energy and microgrid projects already completed or in the works on some military bases. Part II concludes with an assessment of how well the current mandates and solutions are working, and whether those solutions are in line with the stated goal of this paper. Part III focuses on the practical and regulatory challenges faced by the DoD in reaching its goals of security and sustainability. Both environmental and procurement regulations will be examined and analyzed, as will be the notion of "military exceptionalism." Regulatory and practical roadblocks to future success will be identified.

Finally, Part IV will propose solutions to the threat faced by the DoD. It also contains a discussion of needed reforms, including recommendations that the DoD engage in a proper risk assessment of its critical facilities, that energy security should become a more prominent factor in renewable energy acquisitions, and that both Congress and DoD ultimately adopt an "all of the above" solution to the issue of energy security, including the possibility of small-scale nuclear power generation on select DoD installations, in order for the DoD to truly go "off the grid." This Article concludes by discussing the alignment of two political interests in order to resolve the threat. Although the two overlapping interests—national security and environmental protection—traditionally rest at opposite sides of the political spectrum, the possibility of reaching consensus, rarely achievable in today's political environment, will additionally be explored.

I. The Threat

> *We're facing the possibility of an electronic Pearl Harbor . . . There is going to be an electronic attack on this country some time in the future . . . .*
>
> —Deputy Secretary of Defense John Hamre, 1997
>
> *The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack . . . The collective result of these kinds of attacks could be a cyber Pearl Harbor . . . An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches . . . they could . . . shut down the power grid across large parts of the country.*[29]
>
> —Secretary of Defense Leon Panetta, 2012

Our Nation's electricity infrastructure is crucial to our economic success, our security, and sustaining the American way of life.[30] Everything from essential goods and services to communications, food, and water relies upon the commercial power grid.[31] But, the most important function that relies on the commercial power grid is, of course, our Nation's defense.[32] Because of the many diverse threats

24. "Microgrids are localized grids that can disconnect from the traditional grid to operate autonomously. Because they are able to operate while the main grid is down, microgrids can strengthen grid resilience and help mitigate grid disturbances as well as function as a grid resource for faster system response and recovery." *The Role of Microgrids in Helping to Advance the Nation's Energy System*, U.S. Dep't Energy [hereinafter DOE Microgrid], http://energy.gov/oe/services/technology-development/smart-grid/role-microgrids-helping-advance-nation-s-energy-system (last visited May 30, 2016).
25. *See* Tommey, *supra* note 23, at 620 ("The increasing use of smart grid and microgrid technologies, combined with a shift from centralized energy generation to decentralized, small scale facilities better fits the structure and geographic distribution of Department of Defense installations.") (citing Jeff St. John, *The Military Microgrid as Smart Grid Asset*, GreenTech Media (May 17, 2013), http://www.greentechmedia.com/articles/read/the-military-microgrid-as-smart-grid-asset)).
26. *See* Light, *supra* note 23, at 881 (The fact that the DoD "is the largest single consumer of energy in the nation" should be "viewed as an exceptional opportunity for innovation in energy efficiency and the development of new technologies—both of which could have the potential for widespread crossover to and from the civilian realm."); *see also* Tommey, *supra* note 23, at 599 ("[T]he structure and reach of the [DoD] makes it perhaps the most well positioned federal agency to move for sweeping changes in energy management.").
27. U.S. Dep't of Def., Annual Energy Management Report Fiscal Year 2014, at 17 (2015) [hereinafter U.S. Dep't of Def., Energy Management Report FY 2014], http://www.acq.osd.mil/eie/Downloads/Reports/ Tab%20B%20-%20FY%202014%20AEMR_FINAL.pdf ("The Department's FY 2014 facility energy consumption amounted to 1.2 percent of the total U.S. commercial sector's energy consumption. The Department's total energy bill was $18.2 billion.").
28. Light, *supra* note 23, at 900 ("[M]ilitary-supported innovation led to significant civilian 'spillover' which ultimately overtook military sales and funding for R&D."). "[T]he scale of government procurement and R&D in the Cold War permitted greater experimentation, diversity, and competition among industrial partners in technology development." *Id.* at 900 n.113 (citing David C. Mowery, *Defense-Related R&D as a Model for "Grand Challenges" Technology Policies*, 41 Res. Pol'y 1703, 1709 (2012)).
29. Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. Times, Oct. 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.
30. Strategic Plan, *supra* note 19, at 2.
31. *Id.*
32. Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 18; *see also* U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 7 ("Both at installations and in combat platforms, energy is a critical resource and vulnerability across the full range of military operations.").

against the commercial power grid, the DoD's heavy reliance on the grid for both its installation and operational energy needs must change.

A. The Vulnerability of the Commercial Power Grid

Unlike the interstate highway system, the commercial power transmission grid was not built in conformity with a master plan.[33] Rather, it is a patchwork of systems constructed by individual utilities as "isolated transmission islands" to meet local needs.[34] These small networks created by individual utilities were "unsystematically linked when [those] utilities decided to jointly own power plants or to connect to neighboring companies to facilitate power sales."[35] The commercial grid as we know it is made up of three major "interconnections," which includes the Eastern, Western, and Electric Reliability Council of Texas interconnections (the latter which covers most, but not all, of the state of Texas).[36] Thus, the 48 contiguous states essentially have 3 smaller, separate grids with limited connections.[37] Within each of these interconnections, 130 balancing authorities operate a given portion of the grid system.[38] All told, the grid is "owned by several hundred private and public entities."[39]

Because of its patchwork nature, the grid is fragile, therefore making it susceptible to extended outages from natural disasters or sabotage.[40] Essential services, including telecommunications, water supplies and treatment, and the operation of pipelines that distribute oil and natural gas, are interconnected with and interdependent of the commercial power grid.[41] Yet, in the event of a grid failure, these critical services are required for both recovery and continued operation of the power grid.[42] Thus, a prolonged interruption in the power grid could result in a "cascading" failure of other vital infrastructure, including the supply of petroleum and natural gas.[43]

As recently as 2014, Admiral William Gortney, the former head of U.S. Northern Command, the military organization charged with defending the U.S. homeland,[44] stated in a press briefing, "All of our—those critical infrastructures are—fragile. And when I say fragile, it's just because we really don't know the true vulnerabilities. We try and mitigate them as best we can. But it causes me great concern."[45] In response to a question from the press about the grid's vulnerability specifically, the Admiral used an example: "[I]f the power grid up in Ottawa fails, then we—that could take the northeast quadrant of the United States out."[46]

According to a comprehensive report by the Defense Science Board ("DSB"),[47] there are four primary sources of risk for grid outages: Sabotage or terrorist activity (including cyber-attacks), overload, natural disasters, and interruptions in supplies to generating plants.[48] Others have pointed to a fifth, though arguably less likely, risk: An electromagnetic pulse ("EMP") attack.[49] In part because of recent media attention, chief among these threats in the eyes of many officials is the threat of a cyber-attack.[50]

The Department of Homeland Security ("DHS"), in its most recent National Infrastructure Protection Plan ("NIPP"), stated that critical infrastructure that has long been subject to risks associated with both physical threats and natural disasters is now more and more exposed to cyber

33. Stan Mark Kaplan, Cong. Research Serv., R40511, Electric Power Transmission: Background and Policy Issues 2 (2009), http://research.policyarchive.org/18743.pdf.
34. *Id.*; *see also* Valerie Volcovici, *Washington Blackout Highlighted Aging Electrical Grid*, Reuters (Apr. 9, 2015), http://www.reuters.com/article/us-usa-grid-blackout-idUSKBN0N02HB20150409 ("If Thomas Edison came back and saw the electric grid, he would still recognize it").
35. Kaplan, *supra* note 33, at 2–3 (noting, however, that as "recently as 1962 the systems that now constitute the Eastern Interconnection were not fully connected . . . .").
36. *Id.* at 3.
37. *Id.*
38. U.S. Dep't of Energy, DOE/GO-102008-2567, 20% Wind Energy by 2030: Increasing Wind Energy's Contribution to U.S. Electricity Supply 91 (2008), http://energy.gov/sites/prod/files/2013/12/f5/41869.pdf.
39. Kaplan, *supra* note 33, at 4.
40. *See* Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 11, 55 ("The grid is a relatively easy target for a terrorist. It is brittle, increasingly centralized, capacity-strained, and largely unprotected from physical attack, with little stockpiling of critical hardware.").
41. *Id.* at 12.
42. *Id.*
43. *Id.*; *see also* David E. Nye, When the Lights Went Out: A History of Blackouts in America 27 (MIT Press ed., 2010) ("As the electrical system extended into every part of daily life, it became the network that underlay all other networks . . . . From water systems, railroads, gas lines, sewer systems and telephone exchanges . . . as reliability and integration increased, so did vulnerability.").
44. U.S. Northern Command "conduct[s] homeland defense, civil support and security cooperation to defend and secure the United States and its interests." *See About USNORTHCOM*, U.S. Northern Command, http://www.northcom.mil/AboutUSNORTHCOM.aspx (last visited May 30, 2016).
45. Press Release, U.S. Dep't of Def., Department of Defense by Admiral Gortney Press Briefing in the Pentagon Briefing Room (Apr. 7, 2015), http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/607034.
46. *Id.*
47. The Secretary of Defense, in accordance with the provisions of the Federal Advisory Committee Act of 1972 (5 U.S.C., Appendix, as amended) and 41 C.F.R. § 102-3.50(d), established the Defense Science Board. The Board's objective is to provide independent advice and recommendations on matters relating to the DoD's scientific and technical enterprises. *See Defense Science Board Charter*, Def. Sci. Board, http://www.acq.osd.mil/dsb/charter.htm (last visited May 30, 2016).
48. Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 55.
49. William C. Anderson, *Energy Security and Microgrids—Protecting Critical Infrastructure from Impacts of Extended Grid Outages*, *in* Renewable Energy for Military Installations: 2014 Industry Review 48 (Am. Council on Renewable Energy ed., 2014), http://acore.org/files/pdfs/Renewable-Energy-for-Military-Installations.pdf. An electromagnetic pulse generated by a high altitude nuclear detonation can cover a continent, exposing communications and other electronic equipment to a potentially damaging or functionally disrupting environment. Carl E. Baum, *From Electromagnetic Pulse to High-Power Electromagnetics*, 80 Procs. IEEE 789 (1992), http://ece-research.unm.edu/summa/notes/SDAN/0032.pdf.
50. *See, e.g.*, Matthew Deluca, *Are We Prepared for a Cyber Attack on the Grid?: Lawmakers*, NBC News, Apr. 14, 2016, http://www.nbcnews.com/tech/tech-news/are-we-prepared-cyber-attack-power-grid-lawmakers-n556001 ("In the [U.S.], there has not yet been a successful cyber attack that has had a widespread impact on infrastructure. Experts and officials including NSA Director Mike Rogers have repeatedly warned of the danger, however."); Bill Gertz, *FBI Warns of Cyber Threat to Electric Grid*, Wash. Free Beacon, Apr. 8, 2016, http://freebeacon.com/issues/fbi-warns-cyber-threat-electric-grid/ ("Three months after a [DHS] intelligence report downplayed the threat of a cyber attack against the U.S. electrical grid, DHS and the FBI began a nationwide program warning of the dangers faced by U.S. utilities from damaging cyber attacks like the recent hacking against Ukraine's power grid."); Bill Loveless, *Koppel: Cyber Attack on Power Grid? It's Going to Happen*, USA Today, Feb. 21, 2016, http://www.usatoday.com/story/money/columnist/2016/02/21/koppel-cyber-attack-power-grid-s-going-happen/80614078/ (discussing former newsman Ted Koppel's book, *Lights Out: A Cyberattack, A Nation Unprepared*).

risks.[51] This risk became greater in the last ten years because of the growing integration of information and communications technologies with critical infrastructure operations.[52] In this last decade, there have already been several attempted attacks on the Supervisory Control and Data Acquisition ("SCADA") systems that control the grid, but, luckily, none have yet resulted in major outages.[53]

Former Defense Secretary Panetta, quoted at the beginning of this section, is not the only top U.S. official to sound the alarm about a cyber-attack on the Nation's critical infrastructure.[54] Admiral Michael Rogers, who, since April of 2014, serves the dual role as head of U.S. Cyber Command[55] and the National Security Agency ("NSA"), recently told a Congressional panel that China and "probably one or two other" countries have the ability to completely disrupt the U.S.'s power grid by way of a cyber-attack.[56] Echoing the statements of other government officials in the years prior, Admiral Rogers told the panel that "[i]t is only a matter of the when, not the if, that we are going to see something traumatic."[57] Similarly, the Director of the Central Intelligence Agency ("CIA"), John Brennan, fairly recently stated in a *60 Minutes* interview that a cyber-attack on the Nation's infrastructure "really is the thing that keeps [him] up at night."[58]

Although the U.S. has not yet suffered a cyber-attack on its critical infrastructure,[59] the type of attack that U.S. leaders have warned about was recently carried out against the country of Ukraine. On December 23, 2015, the Ukrainian Kyivoblenergo, which is one of the country's regional electricity distribution companies, suffered a significant service outage due to a cyber-attack.[60] The outages were caused by hackers' entry into the company's computer and SCADA systems, leading to thirty substations being disconnected for several hours.[61] The company was forced to switch to manual mode in order to regain control of its systems, but only after approximately 225,000 customers had already lost power.[62] Two months later, the company's control centers were still not fully operational.[63] In the postmortem analysis, officials highlighted their concern that the hackers were able to "perform long-term reconnaissance operations required to learn the environment and execute a highly synchronized, multistage, multisite attack."[64] Even though the attack resulted in only a temporary power interruption, experts found that the control systems in Ukraine were more secure than some in the U.S.[65] Nonetheless, the Ukrainian systems were still insufficient to thwart the attack.

As others have rightly pointed out,[66] it is not just a cyber-attack that could potentially incapacitate the grid. On August 14, 2003, large portions of the Midwest and Northeast United States, as well as parts of Canada, experienced a complete blackout due to cascading system failures within the grid.[67] One of the top ten power outages in world history, it impacted an area with nearly 50 million people and 61,800 megawatts ("MW")[68] of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey, and the Canadian province of Ontario.[69] Power was not restored for 4 days in several

51. U.S. Dep't of Homeland Sec., National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security & Resilience 8 (2013).
52. *Id.*
53. *See* Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 20, 55, 118 ("SCADA systems are used in utility infrastructures as a computer-based monitoring and control system that centrally collects, displays, and stores information from remotely-located data collection transducers and sensors to support the control of equipment, devices, and automated functions.").
54. *See* Bumiller & Shanker, *supra* note 29.
55. U.S. Cyber Command is an armed forces sub-unified command, which is subordinate to the larger U.S. Strategic Command ("USSTRATCOM"). Its mission is to plan, coordinate, integrate, synchronize, and conduct activities to "direct the operations and defense of specified [DoD] information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to [its] adversaries." *See U.S. Cyber Command*, U.S. Strategic Command (May 2016), https://www.stratcom.mil/factsheets/2/Cyber_Command/.
56. Jamie Crawford, *The U.S. Government Thinks China Could Take Down the Power Grid*, CNN, Nov. 21, 2014, http://www.cnn.com/2014/11/20/politics/nsa-china-power-grid/.
57. *Id.*
58. John Brennan, *Interview on 60 Minutes*, CBS News, Feb. 14, 2015, http://www.cbsnews.com/news/cia-director-john-brennan-60-minutes-scott-pelley/.
59. *See, e.g.*, U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 44 ("No malicious acts (e.g., physical, cyber) were reported as causing utility outages impacting installations in FY 2012, FY 2013, or FY 2014."); *see also* U.S. Dep't of Def., Annual Energy Management Report Fiscal Year 2015, at 46 (2015) [hereinafter U.S. Dep't of Def., Energy Management Report FY 2015] (no malicious acts were reported in FY 2015 either), http://www.acq.osd.mil/eie/Downloads/IE/FY%202015%20AEMR.pdf.
60. Elec. Info. Sharing & Analysis Ctr., Analysis of the Cyber Attack on the Ukrainian Power Grid 1 (2016) [hereinafter E-ISAC Report], http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf ("Shortly after the attack, Ukrainian government officials claimed the outages were caused by a cyber-attack, and that Russian security services were responsible for the incidents.").
61. *Id.*
62. *Id.*
63. Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, Wired, Mar. 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (citing Press Release, Indus. Control Sys. Cyber Emergency Response Team, U.S. Dep't of Homeland Sec., Alert (IR-ALERT-H-16-056-01): Cyber Attack Against Ukrainian Critical Infrastructure (Feb. 25, 2016), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01).
64. E-ISAC Report, *supra* note 60, at 4–5, 23 ("[T]he adversaries demonstrated the capability and willingness to target field devices at substations, write custom malicious firmware, and render the devices, such as serial-to-ethernet convertors, inoperable and unrecoverable.").
65. Zetter, *supra* note 63.
66. *See* Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 54–56.
67. U.S.–Canada Power Sys. Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations 1 (2004) [hereinafter Report on 2003 Blackout], http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.
68. One kilowatt ("kW") equals 1000 watts. One kilowatt-hour ("kWh") is one hour of using electricity at a rate of 1000 watts. As an example, an energy-efficient refrigerator uses about 300-400 kWh per year. The typical American home uses about 7200 kWh of electricity each year. Megawatts ("MW"), on the other hand, are used to measure the output of a power plant or the amount of electricity required by an entire city. One megawatt ("MW") equals 1000 kW, which equals 1,000,000 watts. For example, a typical coal plant is about 600 MW in size. The final relevant metric here, gigawatts (not "jigawatts," with all due respect to the fictional Doctor Emmett Brown), measure the capacity of large power plants. One gigawatt ("GW") equals 1000 MW, which equals 1 billion watts. *See How is Electricity Measured?*, Union Concerned Scientists, http://www.ucsusa.org/clean_energy/our-energy-choices/how-is-electricity-measured.html#.V0EODZErLic (last visited May 30, 2016); *see also* Back to the Future (Universal Pictures 1985) (referring to a "bolt of lightning" being equal to 1.21 "jigawatts").
69. Report on 2003 Blackout, *supra* note 67, at 1.

parts of the Eastern United States, while Ontario, Canada, suffered rolling blackouts for over a week before full power was restored.[70]

In 2005, the now infamous Hurricane Katrina devastated regional power infrastructure in Louisiana, Mississippi, and Alabama, leaving approximately 2.5 million Americans without electricity; some customers were left without power for weeks.[71] In October 2012, when "Superstorm" Sandy hit the East Coast, it left more than eight million customers in seventeen states without any power.[72]

More than one million of those customers did not see service restored until over a week had passed.[73] And, as recently as April 2015, Washington D.C. itself, including the White House, the State Department, and, ironically, the Department of Energy ("DOE"), in addition to large swaths of southern Maryland, lost power when a lone transmission line in Maryland was severed.[74] With respect to the threat against the power grid, a minority of industry and government officials have responded, "so what?"[75] Although DHS has since changed its tune after the recent Ukrainian grid attack,[76] the argument among these officials was essentially that the likelihood of a successful attack on the grid—whether it be a cyber or physical attack—is low.[77] Despite this being the minority view, the opinion that the threat to the grid should be disregarded because the risk is too low should itself be viewed with a great deal of skepticism. As the DSB warned, "[f]rom a commercial utility's perspective, risk mitigation actions such as hardening facilities and systems . . . incur significant costs that it may not be possible to fully pass on to customers."[78] This economic disincentive is one of the reasons why the grid currently "is not as secure as it could or should be."[79] These cost considerations also likely to color much of the industry skeptics' point of view.[80]

As regards the few government officials that have expressed doubt about the growing threat, the vast majority of top officials in the field or with specialized expertise in the area agree that, even if one assumes the risk of an attack is relatively low, the impact of an attack could be catastrophic.[81] The risk is so serious that in October 2015, President Obama himself warned that the U.S. was failing to dedicate enough resources to the threat against the power grid.[82] The President stated that "[n]ot only is it a threat to our national security, but failing to maintain and strengthen our infrastructure also jeopardizes our economic growth and closes doors of opportunity for all our citizens."[83]

Ultimately, some of the best predictors of actual risk and potential cost are in the insurance industry.[84] Lloyd's of London,[85] together with the University of Cambridge Centre for Risk Studies, recently released a report concerning the insurance implications of a wide-scale cyber-attack on the U.S. grid.[86] The report hypothesized a scenario in which a Stuxnet-style[87] cyberattack plunges fifteen states, including New York and the District of Columbia, into darkness and leaves 93 million people without power.[88] Though the study found that such a widespread cyber-attack was improbable, it did find that it was technologically possible.[89] The economic damages, including direct damage to assets and infrastruc-

70. *Id.*
71. White House, The Federal Response to Hurricane Katrina: Lessons Learned 28, 61 (2006), http://www.disastersrus.org/katrina/White%20House%20Katrina%20report.pdf.
72. Kayla Webley, *Hurricane Sandy by the Numbers: A Superstorm's Statistics, One Month Later*, Time, Nov. 26, 2012, http://nation.time.com/2012/11/26/hurricane-sandy-one-month-later/.
73. Alan Taylor, *Hurricane Sandy: One Week After Landfall*, Atlantic, Nov. 5, 2012, http://www.theatlantic.com/photo/2012/11/hurricane-sandy-one-week-after-landfall/100399/; *see also* Volcovici, *supra* note 34 ("One of the things being worked on now is a significant effort resulting from Superstorm Sandy to improve the resilience of the grid.").
74. Nicole Gaouette & Justin Sink, *State Department, White House Lose Electricity in Washington*, Bloomberg, Apr. 7, 2015, http://www.bloomberg.com/politics/articles/2015-04-07/state-department-white-house-lose-power-in-washington-outages.
75. *See, e.g.*, Kate Bo Williams, *DHS: Risk of Destructive Cyber Attack on Grid "Low"*, Hill, Apr. 6, 2016, http://thehill.com/policy/cybersecurity/275370-dhs-risk-of-destructive-cyberattack-on-grid-low (According to a leaked DHS report, "The majority of malicious activity occurring against the U.S. energy sector is low-level cybercrime that is likely opportunistic in nature rather than specifically aimed at the sector . . . and is not meant to be destructive.").
76. *See* Gertz, *supra* note 50.
77. Williams, *supra* note 75.
78. Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 57.
79. *Id.* at 57.
80. *See* Rebecca Smith, *Proposal to Prevent Grid Attack Lacks Power, Critics Say*, Wall St. J., Apr. 17, 2014, http://www.wsj.com/articles/SB10001424052702304626304579507772912641760 ("[D]raft regulations—written by the power industry—are drawing criticism from experts who say the proposals are too loose to stop saboteurs"). *But see* Aaron Boyd, *Energy Awards $35M to Protect Power Grid From Cyber Attacks*, Fed. Times, Oct. 13, 2015, at 1, 2, http://www.federaltimes.com/story/government/cybersecurity/2015/10/13/power-grid-cybersecurity/73883364/ (After the Department of Energy awarded two grants totaling $34.7 million to the cause, David Nicol, director of UI's Information Trust Institute and principal investigator for the Cyber Resilient Energy Delivery Consortium, stated: "We need to be able to integrate advanced cyber components with the assurance that we aren't making systems more vulnerable.").
81. *See, e.g.*, Bumiller & Shanker, *supra* note 29 (former Defense Secretary Panetta); Crawford, *supra* note 56 (current NSA Director Admiral Rogers); Steve Reilly, *Bracing for a Big Grid Attack: 'One is too Many'*, USA Today, Mar. 24, 2015, http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/ ("It's one of those things: One is too many, so that's why we have to pay attention," said FERC Chairman Cheryl LaFleur); Smith, *Assault on California Power Station Raises Alarm on Potential for Terrorism*, *supra* note 1, at 4 (former FERC Director Wellinghoff, director of Consolidated Edison Inc. and FBI veteran Michelle Campanella).
82. Press Release, The White House, Presidential Proclamation—Critical Infrastructure Security and Resilience Month, 2015 (Oct. 29, 2015), https://www.whitehouse.gov/the-press-office/2015/10/29/presidential-proclamation-critical-infrastructure-security-and.
83. *Id.*
84. The DOE's recent actions are a good indication of the risk, too. *See, e.g.*, Boyd, *supra* note 80, at 1 ("The Department of Energy awarded two research grants totaling $34.7 million to develop cybersecurity tools and standards to protect the nation's electricity infrastructure.").
85. *See* Lloyd's, Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid at "About Lloyd's" (2015) [hereinafter Lloyd's, Business Blackout] ("Lloyd's is the world's only specialist insurance and reinsurance market that offers a unique concentration of expertise and talent, backed by strong financial ratings and international licenses [sic]. It is often the first to insure new, unusual or complex risks, providing innovative insurance solutions for local, cross border and global risks.").
86. *See id.* at 4.
87. *Id.* at 46 (Stuxnet was a malicious computer code used by an unknown nation state that targeted an industrial control system ("ICS") at an Iranian nuclear plant).
88. *Id.* at 4 ("The scenario predicts a rise in mortality rates as health and safety systems fail; a decline in trade as ports shut down; disruption to water supplies as electric pumps fail and chaos to transport networks as infrastructure collapses.").
89. *Id.*

ture, as well as the decline in sales revenue to electricity supply companies and to businesses, was estimated to be $243 billion, "rising to more than $1 trillion in the most extreme version of the scenario."[90] And, referencing the aforementioned PG&E incident, among others, the report concluded that a relatively small team of attackers would be able to carry out the widespread and costly attack.[91]

B. The DoD's Risk

The DoD almost exclusively relies on the commercial power grid for both its installation[92] and operational energy[93] requirements. In 2008, the DSB found that 99% of the electrical energy that DoD consumed originated "outside the fence"—that is, from sources outside of DoD installations.[94] Moreover, the DoD's most critical assets—those assets specifically identified by the agency as absolutely necessary for defense purposes—are vulnerable to disruptions in the electrical power supply.[95] A total of thirty-one out of the thirty-four most critical DoD assets rely on the commercial power grid.[96] Of those thirty-one assets, twenty-four have, at one point in time, experienced a significant power outage.[97] Due to this reliance, the DSB sounded the alarm that essential national security and homeland defense facilities and missions faced an unacceptably high likelihood of an extended outage.[98]

In the years since the DSB's oft-cited 2008 report, the DoD's reliance on the commercial grid has not significantly decreased.[99] Despite the fact that there has been a shift towards the department using more and more renewable energy sources, the reliance on the commercial grid persists. This reliance is particularly dangerous because DoD installations serve a number of important purposes, both domestically and abroad. For example, many of the Nation's land-based defensive and offensive ballistic missile systems are located on domestic military bases;[100] military installations increasingly act as a base for emergency services after natural or human caused disasters;[101] during contingency operations, unmanned aerial vehicles are frequently piloted from U.S.-based installations;[102] and highly critical missions around the world depend on domestic bases' command, control, communications, computers, intelligence, surveillance, and reconnaissance ("C4ISR") capabilities.[103] As the DoD itself recognized in the 2015 sustainability report, "[w]ith the increasing reliance of U.S. combat forces on 'reach back' support from installations in the [U.S.], power failure at those installations could adversely affect power projection and homeland defense capability . . . an energy threat to [domestic] bases . . . can be a threat to operations abroad."[104]

It is true that many military installations, including the DoD's most critical facilities, have backup power from fossil fuel-based generators.[105] Fossil fuel powered generators, however, are only designed to keep basic installation functions and critical missions operating for an average of 3 to 7 days.[106] Further, diesel generators are just as susceptible to long-term interruptions because of limited fuel, in addition to the potential vulnerability of the fuel delivery infrastructure in the event of a power disruption.[107] This backup generator approach was based on the assumption that commercial power was, by and large, reliable, and that the backup generators could meet demand.[108] But, as DoD has now recognized,[109] its previous assumptions regarding the reliability of commercial power no longer hold true, and it thus has to take a more rigorous, risk-based approach to ensure its critical missions are protected.[110]

The DoD manages over 500 installations worldwide, including nearly 300,000 buildings.[111] It is the single larg-

90. Lloyd's, Business Blackout, *supra* note 85, at 4.
91. *Id.* at 4, 45–46 (included in Annex A of the Report is a list of cyber-attacks against industrial control systems since 1999).
92. The term "installation" or "facility energy" includes "energy needed to power fixed installations and enduring locations as well as non-tactical vehicles." U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 8.
93. The term "operational energy" means the "energy required for training, moving, and sustaining military forces and weapons platforms for military operations. The term includes energy used by tactical power systems and generators and weapons platforms." 10 U.S.C. § 2924(5) (2012).
94. Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 18 (citation omitted).
95. U.S. Gov't Accountability Off., GAO-10-147, Defense Critical Infrastructure: Actions Needed to Improve the Identification & Management of Electrical Power Risks and Vulnerabilities to DoD Critical Assets 6 (2009) [hereinafter Defense Critical Infrastructure GAO Report 2009], http://www.gao.gov/new.items/d10147.pdf.
96. *Id.*
97. Andrea Marr & Wilson Rickerson, Generating Security: Resilient, Renewable Power for U.S. Military Installations 12 n.3 (2014), http://cnponline.org/wp-content/uploads/2014/04/Generating-Security-Resiliant-Renewable-Power-for-U.S.-Military-Installations1.pdf (referencing Defense Critical Infrastructure GAO Report 2009, *supra* note 95).
98. Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 63.
99. *See, e.g.*, *Before the Subcomm. on Energy & Power, Comm. Energy & Commerce, & H.R.*, 112th Cong. 1 (2011) (testimony of Honorable Paul Stockton, Assistant Secretary of Defense, Homeland Defense and Americas' Security Affairs Department of Defense) ("The [DoD] relies on commercial power for nearly 99% of its power needs at military installations.").
100. CNA Military Advisory Bd., National Security and Assured U.S. Electrical Power 9 (2015), https://www.cna.org/CNA_files/PDF/National-Security-Assured-Electrical-Power.pdf.
101. Constantine Samaras & Henry H. Willis, Capabilities-Based Planning for Energy Security at Department of Defense Installations 1 (Rand Corp. ed., 2013), http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR162/RAND_RR162.pdf; *see also* Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 53 ("As a result, a much larger portion of the installation becomes a critical mission requiring highly reliable power.").
102. Samaras & Willis, *supra* note 101, at 2 (citing Elizabeth Bumiller, *A Day Job Waiting for a Kill Shot a World Away*, N.Y. Times, July 29, 2012, http://www.nytimes.com/2012/07/30/us/drone-pilots-waiting-for-a-kill-shot-7000-miles-away.html?_r=0).
103. *Id.* at 2.
104. U.S. Dep't of Def., Sustainability Performance Report FY 2015, at 1 (2015).
105. Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 53; *see also* Samaras & Willis, *supra* note 101, at 5.
106. Acevedo, *supra* note 23, at 355 n.71 (citing Richard B. Andres & Halla L. Breetz, *Small Nuclear Reactors for Military Installations: Capabilities, Costs, and Technological Implications*, 262 Strategic Forum 1, 3 (2011)); Marr & Rickerson, *supra* note 97, at 6 ("At present, many installations depend on aging back-up power infrastructure and diesel generators that only have a 72-hour fuel supply."); Samaras & Willis, *supra* note 101, at 5 (citing Stockton, *supra* note 99, at 2) ("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.").
107. Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 56, 64.
108. *Id.* at 53.
109. *See* Stockton, *supra* note 99, at 4.
110. Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 53.
111. U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 7. To put this into perspective, this is three times larger than Walmart and

est consumer of energy in the Nation,[112] and its installations consume more than 1% of total energy in the U.S.[113] Nevertheless, not every installation and not every mission requires long-term, islanded[114] backup power. Consequently, the DSC recommended that the DoD accomplish three things in order to prioritize the energy needs of its facilities: "assess the relative risk of power outage at each installation; identify and assess the cost and feasibility of options to satisfy power requirements for the duration of a serious outage; and develop the business case to identify least-cost options for reducing risk to acceptable limits."[115]

Since the DSC's 2008 report, the DoD has been making incremental progress toward better assessing risk and prioritizing its energy needs, yet the dependence on fossil-fuel powered generators nonetheless remains.[116] In a recent promising development, however, officials with the Office of the Assistant Secretary of Defense for Energy, Installations, and Environment ("OASD (EI&E)") reviewed energy resilience data requested from and provided by DoD installations,[117] which were compiled and submitted by each military branch, in order to examine adherence to existing energy resilience policies.[118] Based on its review, the DoD clarified its installation and facility energy policies in order to raise awareness of and prioritize energy resilience requirements.[119]

On March 16, 2016, the department released a changed Department of Defense Instruction ("DoDI") concerning its installation energy management. The Department now mandates that DoD components "clearly define, identify, and update critical energy requirements that align to critical mission operations . . . and incorporate defense critical infrastructure ("DCI") when developing critical energy requirements on military installations . . . ."[120] Additionally, the DoDI makes clear that "[e]nergy resilience solutions are not limited to traditional standby or emergency generators. They can include integrated, distributed, or renewable energy sources" or can include "upgrading, replacing, and maintaining current energy generation systems, infrastructure, and equipment . . . ."[121] Moreover, DoD components are now encouraged to "use alternative financing or utility privatization arrangements in the pursuit of energy resilience projects, when they are life cycle cost effective."[122]

In addition, apparently following the recommendation of the DSC's 2008 report, on April 28, 2015, the then-acting OASD (EI&E), Mr. John Conger, commissioned a study to investigate business case analysis approaches for energy resilience.[123] One of the stated objectives of the study is not just to identify energy projects that improve energy resilience among the services, but also to encourage integrated and holistic energy solutions beyond fossil-fuel powered generators.[124] While not coming right out and stating that the study is analyzing the long-term feasibility and cost-effectiveness of microgrid technology, this nevertheless appears to be the objective of the study. Moreover, the DoD's most recent Energy Management Report[125] states that the department is carrying out The Environmental Security Technology Certification Program ("ESTCP") Installation Test Bed, which "funds microgrid and advanced installation energy management technology demonstrations to evaluate the benefits and risks of various approaches and configurations."[126] This is in addition to the SPIDERS program, which will be discussed in more detail below. Thus, with the DoD moving towards microgrid technology as an option to protect its installations from disruptions in the power supply, it is important to understand how exactly the technology works and what it can provide.

C. *Microgrids: A Likely Solution*

According to the DOE, a microgrid is a localized or "islanded" grid that can disconnect from the traditional grid in order to operate independently, thus mitigating grid disturbances and strengthening energy resilience.[127] Although microgrids generally operate while connected to the commercial grid, they have the capability to break off and operate—island—on their own, using local energy generation in the event of a blackout or power interruption.[128] They can be powered by, among other things, renewable sources like solar panels or wind energy, and have the potential to run indefinitely.[129] "A microgrid connects to the [commercial] grid at a point of

six times greater than the General Services Administration. Andrew Holland et al., Powering Military Bases: DoD's Installation Energy Efforts 2 (2013), https://www.americansecurityproject.org/ASP%20Reports/Ref%20128%20-%20DoD%20Installation%20Energy%20Fact%20Sheet.pdf.

112. Marr & Rickerson, *supra* note 97, at 2.
113. Holland et al., *supra* note 111, at 1.
114. "Islanding" allows a facility to shed non-essential electrical loads and maintain mission-critical loads if the electrical grid is disrupted. U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 113.
115. Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 58.
116. U.S. Gov't Accountability Off., GAO-15-749, Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning 32–34 (2015) [hereinafter DOD Reporting GAO Report 2015].
117. *See* Memorandum from John Crager, Assistant of the Sec'y of Def. (Energy, Installations and Env't), to Assistant Sec'y of the Navy (Installations, Energy and Environment) et al. (Apr. 28, 2015) [hereinafter Energy Resilience Business Analysis Case Study], http://www.acq.osd.mil/eie/IE/FEP_Energy_Resilience.html; *see also* 10 U.S.C. § 2925 (2012) (requiring that the Secretary of Defense furnish Congress, among other things, "[d]etails of all commercial outages caused by threats and those caused by hazards at military installations that last eight hours or longer, whether or not the outage was mitigated by backup power . . . .").
118. DOD Reporting GAO Report 2015, *supra* note 116, at 35 n.50 ("According to DoD's definition, power resilience is the planning and capability to ensure the department has available, reliable, and high-quality power to continuously accomplish missions from its installations in the face of potential disruptions.").
119. *See generally* U.S. Dep't of Def., Department of Defense Instruction No. 4170.11 (2009) (Change 1, effective Mar. 16, 2016) [hereinafter DoDI 4170.11], http://www.dtic.mil/whs/directives/corres/pdf/417011p.pdf.
120. *Id.* at 16.
121. *Id.*
122. *Id.* at 17.
123. Energy Resilience Business Analysis Case Study, *supra* note 117.
124. *See id.* at Attach. 1.
125. DoD must submit these yearly reports describing its facility energy activities to Congress. *See* 10 U.S.C. § 2925 (2012) (the Energy Management Report mistakenly cites this authority as 10 U.S.C. § 2924 (2012)).
126. U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 47.
127. *See* DOE Microgrid, *supra* note 24.
128. *How Microgrids Work*, U.S. Dep't Energy, http://www.energy.gov/articles/how-microgrids-work (last visited May 30, 2016).
129. *Id.*

common coupling that maintains voltage at the same level as the main grid," but contains a switch that "can separate the microgrid from the main grid automatically or manually, and it then functions as an island."[130] As power needs fluctuate, microgrids also have the potential to either draw electricity from the commercial grid, or to sell the excess power to the local utility.[131]

Closely related to microgrids is the concept of "distributed generation," which is also known as "on-site generation" or "distributed energy."[132] This involves the production of electricity located at or near the end user it serves, which allows the production to be more decentralized, rather than originating from one central point.[133] Distributed generation systems typically consist of a power generating source, an energy storage system, and advanced monitoring interfaces.[134] An added benefit to distributed generation is the fact that the shorter the distance from generation to consumption, the more efficient, economical, and environmentally-friendly the process likely can be.[135] Microgrids can organize distributed generation technology "into a closed, low-voltage system that may address the needs of multiple users using multiple kinds of technologies."[136] Because energy generation does not occur at a single location or from a single power plant, this distributed generation must be managed and ultimately integrated into one comprehensive and reliable energy supply.[137]

Even still, decentralization of power sources assists greatly in achieving energy security. For example, if one power source fails on one microgrid, it ought to have no impact on other power sources on a different grid.[138] Additionally, decentralized microgrids can serve DoD's remote sites very well, where transmission from the main grid is expensive, challenging, or vulnerable to physical attacks.[139] Furthermore, decentralized microgrids typically do not require new parallel infrastructure for other utilities since microgrids are frequently found in areas where such utilities are already extant.[140]

While many DoD installations have on-site renewable energy power resources (to offset electricity purchases from the commercial grid), most of these systems cannot yet provide power to the base in the event of a blackout.[141] The benefit of connecting these systems to a microgrid is that these resources could operate "both in connection with the grid and completely independent of the grid[,]" in addition to providing power "through distributed generation to multiple loads across a military installation."[142] Microgrids can, therefore, harness bases' existing renewable energy resources to substantially extend islanding time in the event of a blackout.[143] Moreover, microgrids have the additional capability to automatically prioritize critical assets on an installation, thus shedding less important uses of power in an emergency.[144]

At bottom, the DoD would see three significant benefits by shifting more towards the use of microgrids on its installations.[145] First, a microgrid's ability to automatically shift power to where and when it is needed will invariably increase overall energy efficiency by reducing energy waste, thus allowing DoD to continue to decrease its electricity use.[146] Second, microgrids will dramatically increase energy security[147] by reducing reliance on the main grid, as well as on fossil-fuel powered generators.[148] Third, because of their "ability to integrate renewable energy sources by handling non-continuous sources of power when they are available, such as wind and solar, a microgrid will facilitate the DoD's renewable energy goals into the future."[149]

II. The Path to Renewable Energy and Microgrid Procurements at DoD

So, how did the DoD get here? How did the department end up at the forefront of an energy and renewable technology transformation? And, has it been successful in leading

130. *Id.*
131. Sara C. Bronin, *Curbing Energy Sprawl With Microgrids*, 43 Conn. L. Rev. 547, 560 (2010).
132. *Id.* at 549 n.5 (citing Mark Rawson, *Distributed Generation Costs and Benefits Issue Paper*, II (2004), http://www.energy.ca.gov/papers/2004-08-30_RAWSON.PDF).
133. *Id.* (citing U.S. Dep't of Energy by Litos Strategic Commc'n, The Smart Grid: An Introduction 18 (2008) [hereinafter Intro to Smart Grids], http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf).
134. Robert Lasseter et al., Integration of Distributed Energy Resources: The CERTS MicroGrid Concept 1 (2003), http://bnrg.eecs.berkeley.edu/~randy/Courses/CS294.F09/MicroGrid.pdf.
135. Intro to Smart Grids, *supra* note 133, at 12.
136. Bronin, *supra* note 131, at 559.
137. Marr & Rickerson, *supra* note 97, at 4.
138. *See* Bronin, *supra* note 131, at 563 (citing Robert Lasseter, *Microgrids and Distributed Generation*, 133 J. Energy Engineering 144, 146 (2007)).
139. *Id.*
140. *Id.* at 561–62.
141. Marr & Rickerson, *supra* note 97, at 4.
142. *Id.*
143. Holland et al., *supra* note 111, at 3; *see also* U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 47 ("Smart microgrids and energy storage offer a more robust and cost-effective approach to ensuring installation energy resilience than the traditional approach of backup generators tied to single critical loads and (limited) supplies of on-site fuel.").
144. Holland et al., *supra* note 111, at 3 ("Microgrids can also improve the resiliency of the civilian power grid by allowing military bases to automatically shut down non-critical systems during commercial demand spikes. This would allow utilities greater flexibility in managing power loads.").
145. *But see* William A. Mogel, *Book Review: Lighting the World*, 36 Energy L.R. 425, 427 (2015) (From the founder and editor-in-chief emeritus of the Energy Law Review: "[T]here are negatives with microgrids. They are expensive to install and maintain, they are not suitable for low density, widespread communities, and they rely on individuals qualified in technology and maintenance and knowledgeable about the needs of the community.").
146. Tommey, *supra* note 23, at 621 (citing U.S. Dep't of Def., Annual Energy Management Report Fiscal Year 2012 (2013)); *see also* U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 47 ("Advanced microgrids reduce installation energy costs on a day-to-day basis by allowing for load balancing and demand response, as well as offering DoD a pathway to participate in ancillary service markets, all of which can make holistic energy management more cost-effective.").
147. Because of their decentralized nature, microgrids make it more difficult for hackers to carry out a sweeping attack on DoD's critical infrastructure. That said, microgrids are not, of course, *per se* impervious to cyber-attacks.
148. Tommey, *supra* note 23, at 621; *see also* U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 47 (Microgrids "also facilitate the incorporation of renewable and other on-site energy generation. More importantly, they offer energy resilience: the combination of on-site energy and storage, together with the microgrid's ability to manage local energy supply and demand, allow installations to operate in 'islanded' mode, shedding non-essential loads and maintaining mission-critical loads if the electrical grid is disrupted.").
149. Tommey, *supra* note 23, at 621–22 (citing Red Mountain Insights, Military Microgrids: Market Potential, Case Studies, Provider Profiles 7 (2013)).

the way towards energy security and sustainability so far? This section will discuss the mandates imposed on the DoD by both the President and Congress concerning the use of renewable energy resources, whether the mandates have been met so far, and whether the mandates have aided in achieving the goal of energy security and resiliency. In addition, this section will review the current microgrid projects the DoD has in the works, and whether those projects have yet borne any fruit.

A. Renewable Energy Mandates

The military's focus on the increased use of renewable energy did not appear out of thin air. Driven primarily by shifting public opinion concerning the issue of climate change,[150] both Congress and the President have instituted a number of renewable energy mandates for federal executive agencies, including, of course, the DoD. Despite the worthy goal of reducing carbon emissions, however, these mandates are generally silent when it comes to increasing energy security and resiliency.[151] Nevertheless, expanded procurement of renewable energy sources is a necessary, although not sufficient, piece of the microgrid solution to DoD's energy security problem. And, as discussed later in this Article, many of the same acquisition vehicles used to secure renewable energy sources for DoD bases may also be useful for the future acquisition of microgrids.

1. Congress

The first major federal law addressing the use of renewable energy in executive agencies was Section 203 of the Energy Policy Act of 2005 ("2005 EPAct").[152] The law required that federal agencies obtain, "to the extent economically feasible and technically practicable . . . " a minimum of 3% of their total electric energy (in any fiscal year) from renewable energy from 2007 through 2009, 5% from 2010 through 2012, and 7.5% for 2013 and each fiscal year thereafter.[153] The Act defined "renewable energy" as "electric energy generated from solar, wind, biomass, landfill gas, ocean . . . geothermal, municipal solid waste, or new hydroelectric generation capacity achieved from increased efficiency or additions of new capacity at an existing hydroelectric project."[154] Although the DoD has been making some progress towards Congress' goal, it has consistently fallen short, as documented in its most recent report to Congress: eligible renewable electricity use as a percentage of total electricity use in Fiscal Year 2014 was just 3.5%.[155]

In the National Defense Authorization Act of 2007 ("2007 NDAA"), Congress specifically singled out the DoD in its pursuit of more renewable energy use. The 2007 NDAA stated that it "shall be the goal of the Department of Defense . . . to produce or procure not less than 25 percent of the total quantity of facility energy it consumes within its facilities during fiscal year 2025 and each fiscal year thereafter from renewable sources . . . ."[156] While the 2005 EPAct requires that the DoD retain renewable energy credits ("RECs")[157] for goal attainment, retaining RECs is not a requirement to meet the 2007 NDAA (10 U.S.C. § 2911(e)) goal.[158] Unlike the 2005 EPAct goal, the DoD is making steady progress towards the 2007 NDAA target: In Fiscal Year 2014, its total renewable energy produced or procured as a percentage of total facility energy was 12.3%, up from 11.8% the year prior.[159] Furthermore, based on the spirit of the 2007 NDAA, the Army and Air Force have each established their own independent goal of deploying one GW of renewable energy on or near their respective installations by Fiscal Year 2025.[160]

In the National Defense Authorization Act of 2012 ("2012 NDAA"), Congress took an additional step in the right direction by redefining "energy security" and clarifying that it is a factor to be considered in DoD energy procurements: "The term 'energy security' means having assured access to reliable supplies of energy and the ability to protect and deliver sufficient energy to meet mission essential requirements."[161] In addition, the NDAA directed the DoD, when selecting facility energy projects using renewable energy sources, to "give favorable consideration to projects that provide power directly to a military facility or into the installation electri-

150. *See, e.g.*, Jason Robert Hull, *Hey Now, Let's Be Social: The Social Cost of Carbon and the Case for Its Inclusion in the Government's Procurement of Electricity*, 13 J. Cont. Mgmt. 41, 43 (2015), http://www.ncmahq.org/docs/default-source/default-document-library/articles/jcm15---article-03 ("In an effort to address the public's concerns with climate change, the Federal Government has initiated a number of internal policies related to renewable energy and climate change that will enable the Federal Government to lead by example and attack these 'easy targets' by reducing the carbon footprint of its federal agencies."); Tommey, *supra* note 23, at 601 ("The renewable-friendly political climate . . . has led to a spectrum of actions—legislation, executive orders, and agency initiatives—to position the federal government as a laboratory for the development and promulgation of renewable energy technologies.").

151. *See* Marr & Rickerson, *supra* note 97, at 3.

152. *See generally* 42 U.S.C. § 15852 (2012).

153. *Id.* § 15852(a).

154. *Id.* § 15852(b).

155. U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at app. D, D–2.

156. 10 U.S.C. § 2911(e)(1)(A) (2012).

157. A REC "means the technology and environmental (non-energy) attributes that represent proof that 1 megawatt-hour ("MWh") of electricity was generated from an eligible renewable energy resource, that can be sold separately from the underlying generic electricity with which they are associated and . . . were produced by sources of renewable energy placed into service within 10 years prior to the start of the fiscal year." Exec. Order No. 13,693, 80 Fed. Reg. 15871, 15880 (Mar. 19, 2015). "RECs are not energy, and if DoD purchases them, they are an expenditure that does not contribute to [its] energy security posture. DoD sees minimal benefit in purchasing RECs beyond assisting with compliance with renewable energy mandates, and in general would prefer to allocate funds directly on energy or projects that produce it." U.S. Dep't of Def., Annual Energy Management Report Fiscal Year 2010, at 27 (2011).

158. U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 27.

159. *Id.* at 35 (as part of the Energy Performance Master Plan in the Fiscal Year 2011 Energy Management Report, the 10 U.S.C. § 2911(e) goal also includes a 15% goal by Fiscal Year 2018); *see also* U.S. Dep't of Def., Annual Energy Management Report Fiscal Year 2013, at 33 (2014).

160. Energy Management Report FY 2014, *supra* note 27, at 35; *see also supra* note 69 (discussing gigawatts).

161. 10 U.S.C. § 2924(3)(A) (2012); *see also* Samaras & Willis, *supra* note 101, at 3 ("The 2012 National Defense Authorization Act redefined DoD energy security . . . .").

cal distribution network."[162] In what sounds like a clear nod to microgrids, the Act continues, "[i]n such cases, projects should be prioritized to provide power for assets critical to mission essential requirements on the installation in the event of a disruption in the commercial grid."[163]

2. The President

In addition to the standards and goals set by Congress, the Executive Branch has taken an active role in setting standards for the agencies within its purview. Presidents Clinton, Bush, and Obama have all made efforts to increase the Executive Branch's use of renewable energy sources. Two fairly recent executive orders—Executive Orders ("EO") 13423 (2007) and 13514 (2009)[164]—signed by Presidents Bush and Obama respectively, set additional goals on top of those set out in the 2005 EPAct and 2007 NDAA. However, both were revoked and superseded by the more stringent EO 13693, which President Obama signed on March 19, 2015.[165] Also revoked and superseded by EO 13693 was the Presidential Memorandum regarding Federal Leadership on Energy Management of December 2013,[166] which had directed that 20% of the energy consumed by each federal agency come from renewables by 2020.[167]

EO 13693 sets new ambitious targets to promote renewable energy use within the federal government. The EO directs that federal agencies "shall, where life-cycle and cost-effective," ensure that, at a minimum, *the percentage of the* ***total amount of building electric energy consumed*** *by the agency that is "****renewable electric energy****"* be not less than 10% in fiscal years 2016 and 2017; not less than 15% in fiscal years 2018 and 2019; not less than 20% in fiscal years 2020 and 2021; not less than 25% in fiscal years 2022 and 2023; and not less than 30% by fiscal year 2025 and each year thereafter.[168]

This is not the only renewable energy target articulated in EO 13693. The EO additionally directs that federal agencies "shall, where life-cycle and cost-effective," ensure that, at a minimum, *the percentage of* ***total amount of building electric energy and thermal energy*** *shall be clean energy, accounted for by "****renewable electric energy****" and "****alternative energy,****"* be not less than 10% in fiscal years 2016 and 2017; not less than 13% in fiscal years 2018 and 2019; not less than 16% in fiscal years 2020 and 2021; not less than 20% in fiscal years 2022 and 2023; and not less than 25% by fiscal year 2025 and each year thereafter.[169]

The highlighted portions of both mandates are important here because of the definitions contained within each section. In the mandate concerned with "total building electric energy consumed," the President dictated that the targeted percentages of energy be met using "renewable electric energy." "Renewable electric energy" is defined in the EO almost exactly as "renewable energy" is defined in the 2005 EPAct: "[E]nergy produced by solar, wind, biomass, landfill gas, ocean . . . geothermal, geothermal heat pumps, microturbines, municipal solid waste, or new hydroelectric generation capacity."[170] Conversely, in the mandate concerning the "total amount of building electric energy and thermal energy," the President permitted the target percentages to be met not just by "renewable electric energy," but also by "alternative energy."[171]

These different definitions may, at first glance, seem insignificant; but, the EO's definition of the additional phrase "alternative energy" bodes well for the future development of both microgrids and newer forms of clean energy. Unlike "renewable electric energy," "alternative energy" is defined in the EO as follows:

> "Alternative energy" means energy generated from technologies and approaches that advance heat sources, including biomass, solar thermal, geothermal, waste heat, and renewable combined heat and power processes; combined heat and power; ***small modular nuclear reactor technologies***; ***fuel cell energy systems***; and energy generation, where active capture and storage of carbon dioxide emissions associated with the energy generation is verified.[172]

Moreover, "'[c]lean energy' means renewable electric energy *and* alternative energy."[173] Because this is the first time Congress or the President has included small modular nuclear reactor ("SMR") technology among clean energy sources, the development is potentially groundbreaking.[174] SMRs generally refer to portable nuclear reactors under 300 MW, which are smaller, cheaper, easier to build, and more safe than conventional nuclear reactors.[175] This technology will be discussed in more detail later in this Article, specifically with regard to the current limitations of traditional

162. 10 U.S.C. § 2924(3)(B) (2012).
163. *Id.*
164. EO 13,423 required that "at least half of the statutorily required renewable energy consumed by [an] agency in a fiscal year comes from new renewable sources" (meaning from renewable generators built after 1999). In addition, "to the extent feasible, the agency [should] implement[] renewable energy generation projects on agency property for agency use." Exec. Order No. 13,423, 72 Fed. Reg. 3,919 (Jan. 26, 2007). EO 13,514 authorized a government-wide greenhouse gas emission reduction goal of 28% below 2008 levels by 2020. Exec. Order 13,514, 74 Fed. Reg. 52,117 (Oct. 8, 2009); *see also Guidance for Federal Greenhouse Gas Accounting and Inventories*, Council on Envtl. Quality, https://www.whitehouse.gov/administration/eop/ceq/sustainability/fed-ghg (last visited Oct. 20, 2016).
165. 80 Fed. Reg. at 15880 ("Executive Order 13,423 of January 24, 2007, is revoked . . . Executive Order 13,514 of October 5, 2009 . . . [is] revoked.").
166. Press Release, The White House, Presidential Memorandum—Federal Leadership on Energy Management (Dec. 5, 2013), https://www.whitehouse.gov/the-press-office/2013/12/05/presidential-memorandum-federal-leadership-energy-management.
167. 80 Fed. Reg. at 15,880.
168. *Id.* at 15,872 (emphasis added).
169. *Id.*
170. *Compare* 42 U.S.C. § 15852(b) (2012), *with* 80 Fed. Reg. at 15,883 ("geothermal heat pumps" and "microturbines" have been added to the 2005 EPAct definition of "renewable energy").
171. 80 Fed. Reg. at 15,872.
172. *Id.* at 15,882 (emphasis added).
173. *Id.* (emphasis added).
174. Matthew Bandyk, *Obama Executive Order Tags Small Modular Reactors as Clean Energy*, S&P Global (Mar. 20, 2016), https://www.snl.com/interactiveX/Article.aspx?CdId=A-31794585-10540&FreeAccess=1 ("[D]evelopers have already looked to the federal government as one of their most important potential customers. A top selling point of SMRs is that they could be conveniently installed to provide secure, reliable power off the civilian grid for sensitive federal government facilities like military bases.").
175. *Id.*

"renewable energy" with microgrids. But, this EO language, along with the additional promotion of fuel cell energy, is a promising step towards the future of self-sustaining, on-site power generating facilities.

Unfortunately, other than the brief language discussing modular nuclear reactors and fuel cells, EO 13693 generally neglects mentioning energy security or resiliency. Nor does the EO discuss microgrid technology. The closest language resembling energy security is the definition of "climate resilient design," which "means to design assets to prepare for, withstand, respond to, or quickly recover from disruptions due to severe weather events and climate change for the intended life of the asset."[176]

3. The DoD's Response

All four military branches have adopted clean energy targets in response to the Presidential and Congressional mandates, and, in most cases, the military's own target goals go above and beyond those imposed from above.[177] It is estimated that 384 megawatts ("MW") of on-base renewable energy had been installed by 2013, and the DoD's renewable energy projects generated over 10 trillion British thermal units ("BTUs") in Fiscal Year 2014.[178] Also in 2014, the DoD possessed over 1130 renewable energy projects in operation, as compared to approximately 900 in Fiscal Year 2013.[179] An additional 1.7 GW worth of renewable energy projects are in the process of being developed in order to be installed by the end of Fiscal Year 2018.[180]

Although the Presidential and Congressional renewable energy mandates generally only mention the issue of energy security briefly or in passing, the DoD itself seems to recognize that microgrid, long-term battery storage, and fuel cell technologies will all help the department reach its renewable energy goals by making future renewable energy projects more cost efficient, reliable, and palatable to the commanders on the ground, who are rightfully concerned about the mission impact of the formidable renewable energy targets. As such, the DoD is moving forward with both the testing and development of microgrid technology for use with renewable energy sources on its installations. The following section will discuss the microgrid projects currently being developed by the DoD.

B. *Projects and Progress So Far*

> *In the event an attack is successful in triggering a significant grid outage, it will be necessary to operate critical national security infrastructure off the grid for extended periods of time. Microgrids provide an excellent platform to operate critical assets utilizing "on-site" electrical power generation over extended periods in isolation from a crippled grid.*[181]
>
> —The Honorable William C. Anderson (former Assistant Secretary of the Air Force for Installations)

As of July 2015, 124 microgrids were in operation across the U.S., with a total capacity of 1169 MW.[182] By 2020, microgrid capacity in the U.S. is projected to exceed 2850 MW—an increase of nearly 145%.[183] Within the DoD, however, cutting across all four services, there are several microgrid projects either currently running or in the works. More than 40 bases have either installed a microgrid, have plans to develop one, or have carried out a preliminary microgrid study.[184] By 2018, the DoD is expected to produce more than 54.8 MW of microgrid capacity, although this is nowhere near enough to secure all of its critical facilities.[185] Nonetheless, the development of these microgrid technologies helps "spur industry growth and demonstrate [the] feasibility for both military and civilian applications through on-base project deployment."[186]

1. SPIDERS

One of the most prominent microgrid projects within the DoD was the recently-completed Smart Power Infrastructure Demonstration for Energy Reliability and Security Programs, otherwise known as "SPIDERS."[187] The SPIDERS

176. 80 Fed. Reg. at 15,882. This is similar to the definition of "resilience" in EO 13,653, which defined it as the "ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions." 78 Fed. Reg. 66,819, 66,824. Resilience is frequently used throughout EO 13,653 to refer to "climate preparedness and resilience" or "resilience to climate change." *Id.* While the capability to be resilient to climate change may also enable energy security in the broader sense, the EO nevertheless neglects to mention the broader concept of energy security.

177. Marr & Rickerson, *supra* note 97, at 3.

178. *Id.* ("Despite this significant investment in renewable energy, these systems generally do not contribute to increased energy security on military installations. Most on-base renewable energy power systems are configured to offset electricity purchases from the grid but cannot provide power to the base during blackouts"); *see also* U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 38.

179. U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 38.

180. *See* Marr & Rickerson, *supra* note 97, at 3–4 ("Energy technologies that use inherently local and renewable fuels, such as wind, solar, biomass, and geothermal power, can provide the greatest degree of energy certainty to military installations and can stretch scarce fossil fuel supplies.").

181. Anderson, *supra* note 49, at 50 (The Honorable William C. (Bill) Anderson preceded this quote with the following scenario: "The overall effect of a successful attack would impact the target area as well as creating stress on other portions of the grid, transmission, and distribution circuits, causing a cascading effect which could lead to widespread power outages, i.e., blackouts. The impacts of the cascading effect can be significantly reduced by the installation of additional spinning reserves along the grid. Technologies such as synchronous condensers and utility-scale storage devices adjust conditions along the grid to reduce the likelihood of significant cascading. However, adding these spinning reserves to the grid is not currently a priority of the government or utilities.").

182. Dan Boyce, *Military Marches Forward with Microgrids*, Inside Energy (July 9, 2015), http://insideenergy.org/2015/07/09/military-marches-forward-with-microgrids/.

183. PEW Charitable Trusts, Distributed Generation: Cleaner, Cheaper, Stronger—Microgrids in the Evolving Power System 2 (2016), http://www.pewtrusts.org/~/media/assets/2016/02/why_and_how_microgrid_technology_is_a_good_power_source.pdf (citing Julia Pyper, *US Microgrid Capacity Will More Than Double by 2020—and Include a Lot More Renewables*, Greentech Media, June 23, 2015, http://www.greentechmedia.com/articles/read/Microgrid-Capacity-Will-More-Than-Double-by-2020).

184. *Id.* at 4 (citing Red Mountain Insights, *supra* note 149, at 26).

185. *Id.*

186. *Id.* at 3.

187. Naval Facilities Eng'g Command, Technology Transition Final Report, Smart Power Infrastructure for Energy Reliability and Security (SPIDERS), Joint Capability Technology Demonstration, at ES–1

Joint Capabilities Technology Demonstration's ("JCTD") objective was to "demonstrate a secure microgrid architecture with the ability to maintain operational surety through secure, reliable, and resilient electric power and generation. The results of the [SPIDERS] JCTD will help inform infrastructure investment decisions at DOD facilities needed to reduce the unacceptably high risk of extended grid outages."[188] In addition to its stated objective, SPIDERS also listed four critical requirements for the project:

1. Protect task-critical assets from loss of power due to cyber-attack.
2. Integrate renewable and other distributed generation to power task-critical assets in times of emergency.
3. Sustain critical operations during prolonged power outages.
4. Manage installation electrical power and consumption efficiency to reduce petroleum demand, carbon "boot print," and cost.[189]

SPIDERS was instituted in three phases. The first phase was a limited demonstration of a "cybersecure microgrid," which was located and tested at Joint Base Pearl Harbor-Hickam ("JBPHH"), Hawaii, from 2012 to 2013. The microgrid at JBPHH consisted of a "single distribution feeder, two electrically isolated loads, two isolated diesel generators, and an isolated photovoltaic ("PV") array."[190] The second phase of SPIDERS was accomplished at the Army base of Fort Carson, Colorado from 2013 to 2014.[191] The microgrid at Fort Carson "consisted of three distribution feeders, seven building loads, three diesel generators, and a 1-megawatt segment of an onsite PV array, as well as five bidirectional electric vehicle chargers."[192] The third and final phase was conducted at Camp Smith, Hawaii, and was completed in late 2015. This microgrid used "new and existing generation sources . . . to support the loads of the complete installation," in addition to including "stationary prime power diesel generators."[193]

Although SPIDERS used diesel generators to supplement the renewable energy sources in the demonstration, data indicated that the SPIDERS program may be able to achieve a 30% fossil fuel reduction for those generators during power outages.[194] More importantly, the demonstration met all of its stated objections.[195] The Final Report for the SPIDERS program concluded that "[i]ntegrating the outcomes of SPIDERS Phases 1, 2, and 3 into future [DoD] microgrid designs increases the value and security of microgrids at military installations."[196]

2. Environmental Security Technical Certification Program

The ESTCP Installation Energy Test Bed ("IETB"), as mentioned in Part II, is similar to SPIDERS in that it "funds microgrid and advanced installation energy management technology demonstrations."[197] Unlike SPIDERS, the ESTCP IETB is not exclusively dedicated to developing microgrid technology. But, the program provides $30 million in grant money each year to fund environmentally-friendly test programs across the DoD.[198] For example, at Marine Corps Air Station ("MCAS") Miramar, the test bed program funded a cybersecure microgrid and state-of-the-art flow battery backup system, produced by Raytheon and Primus Power, respectively.[199] The microgrid uses a combination of PV arrays, Miramar's gas landfill system, as well as a set of clean-burning diesel generators.[200]

ESTCP also recently awarded a $6 million grant to provide Otis Air National Guard Base in Cape Cod, Massachusetts with a microgrid.[201] Like the MCAS Miramar project, the Otis ANG base microgrid will be constructed by Raytheon and will serve as a test-case for future microgrid projects.[202] The Otis ANG base project is innovative in that it will rely almost exclusively on renewable energy, including a solar array and several wind turbines.[203] And, in order to compensate for the renewable sources' power intermittency (when the wind isn't blowing or the sun isn't shining), high capacity storage batteries will provide stability.[204] Like the other projects mentioned so far, the Otis ANG base microgrid will also include a backup generator, "ready to switch on instantly and protect from outages."[205] Once the microgrid is up and running, the ANG base will have the capability to completely remove itself from the grid.[206]

(2015) [hereinafter SPIDERS Final Report], http://energy.gov/sites/prod/files/2016/03/f30/spiders_final_report.pdf.

188. *Id.* The JCTD initiative is under the co-sponsorship of the DoD, DOE, and DHS.
189. *Id.*
190. *Id.*
191. *Id.* at ES–2.
192. SPIDERS Final Report, *supra* note 187, at ES–2 (bidirectional electric vehicle chargers allows vehicle batteries, charged overnight, to act as power sources for the base during the day).
193. *Id.*
194. *Id.* at 4–1.
195. *Id.*
196. *Id.*
197. U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 47.
198. Marr & Rickerson, *supra* note 97, at 5.
199. Raytheon, *Marines Go Green With Alternative Energy Tech*, Hill (July 7, 2015, 11:50 PM), http://thehill.com/sponsored/content/246588-marines-go-green-with-alternative-energy-tech.
200. Christopher Johns, *Energy Assurance Only a Microgrid Away*, Marines (Jan. 14, 2014), http://www.miramar.marines.mil/News/NewsArticleDisplay/tabid/15785/Article/547849/energy-assurance-only-microgrid-away.aspx.
201. *Military Microgrid to Make Cape Cod Air Force Station Self Sufficient*, Microgrid Knowledge (Dec. 10, 2015), https://microgridknowledge.com/military-microgrid-maked-base-self-sufficient/.
202. *Id.*
203. *Id.*; *see* David Altman Raytheon, *Hybrid Microgrid With High Penetration Wind for Islanding and High Value*, Strategic Envtl. Res. Dev. Program–Envtl. Security Tech. Certification Program [hereinafter Raytheon, *Hybrid Microgrid With High Penetration Wind for Islanding and High Value*], https://www.serdp-estcp.org/Program-Areas/Energy-and-Water/Energy/Microgrids-and-Storage/EW-201606 (last visited Oct. 20, 2016).
204. Raytheon, *Hybrid Microgrid With High Penetration Wind for Islanding and High Value, supra* note 203.
205. *Military Microgrid to Make Cape Cod Air Force Station Self Sufficient*, *supra* note 201.
206. *Id.*

3. Twentynine Palms

Outside of the SPIDERS and ESTCP demonstration programs, several other DoD bases are developing their own microgrids. For example, General Electric recently installed a microgrid at the isolated Marine Corps Air Ground Combat Center Twentynine Palms in the Mojave Desert of California. The base, which supports a population of 22,000 spread across 1000 square miles of desert, typically purchases its power from Southern California Edison, the primary electricity supply company for much of Southern California.[207] Its microgrid, however, will allow the base to "operate even if there is a blackout, using a system of small power plants, solar panels, batteries and diesel generators."[208]

Additionally, the installation's remote and harsh conditions allow it to be an ideal test bed for deployable microgrids—that is, for microgrids used to power forward operating bases ("FOBs") in future combat operations. And, similar to the SPIDERS and ESTCP projects, the Twentynine Palms microgrid will eventually include a "Sodium-Metal-Halide Battery, which can function in the extreme desert climate of Twenty-nine Palms, to help alleviate renewable energy intermittency, improve island-mode operations if the main grid goes down, reduce expensive 'demand changes,' and reduce stress on the main transformers and other electric equipment on base."[209]

4. The Results

The Army is making significant investments in microgrids at Fort Hunter Ligget, Fort Bliss, Fort Sill, Fort Bragg,[210] and Fort Drum.[211] The Navy has microgrid projects underway at its Mobile Utilities Support Equipment Facility in Port Hueneme, California,[212] Naval Submarine Base New London in Groton, Connecticut,[213] and Naval Base Coronado in San Diego, California.[214] Not to be outdone, the Air Force has established its own "Resilient Energy Demonstration Initiative," in order to "develop and deploy innovative energy resilience technologies and business models, and then apply the results to other missions and installations across the Air Force enterprise."[215] The Air Force selected Beale Air Force Base near Sacramento, California to begin developing a test program to provide, "resilient, cost-effective, cleaner power to the installation, and begin implementing that plan by the end of 2016."[216]

Although it is promising that several microgrid projects are being tested and demonstrated across the services, some significant challenges remain. One of the major issues so far is the microgrids' continued reliance on diesel generators, which typically have a supply of only 1 to 3 days' worth of fuel, are connected to loads at the building level (meaning the facilities operator does not have the capability to reroute power to a specific part of a building or to a different building), and are unable to provide continuous power due to their typical thirty-second warm up time. The intermittency of many of the renewable sources that help power the microgrids present a related problem. But, despite these issues, the projects so far (particularly the now-completed SPIDERS initiative) demonstrate unequivocally that microgrids work, that they have tremendous potential to provide energy security to the DoD, and that, therefore, they should be instituted on a larger scale. The next section discusses the regulatory and practical issues that may impede widespread implementation.

III. Green Energy, Red Tape: Regulatory and Practical Challenges

Contrary to what some think, in the vast majority of its actions, the military is not generally exempt from following environmental statutes or regulations.[217] Nor is the DoD allowed to ignore federal procurement regulations, even under

207. U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 48.

208. Rebecca Smith, *Hacker, Terrorist Threats Spur Bases to Build Power Grids*, Wall St. J. (Oct. 21, 2014, 3:42 PM) [hereinafter Smith, *Hacker*], http://www.wsj.com/articles/hacker-terrorist-threats-spur-bases-to-build-power-grids-1413920177.

209. U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 48–49 ("The base sustains its mission with more than 10 MW of power generated on-site by a 1.2 MW solar PV farm, 1 MW of solar PV shading, a 0.5 MW fuel cell, and a 7.2 MW co-generation plant.").

210. Smith, *Hacker*, *supra* note 208.

211. U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 51.

212. Andrew Burger, *New Navy Smart Microgrid Project Will Test Vanadium Flow Battery Storage*, Renewable Energy World (Dec. 2, 2014), http://www.renewableenergyworld.com/articles/2014/12/new-navy-smart-microgrid-project-will-test-vanadium-flow-battery-storage.html; *see also* U.S. Dep't of Def., Energy Management Report FY 2014, *supra* note 27, at 52.

213. *See* Lisa Cohn, *Connecticut Plans 13-MW Naval Base Microgrid; Includes Nearby Community*, Microgrid Knowledge (Dec. 21, 2015), https://microgridknowledge.com/naval_base_microgrid/.

214. *See* Jeff St. John, *The Military Connects Microgrids for a "Secure Cluster" of Power Networks*, Greentech Media (Aug. 26, 2013), http://www.greentechmedia.com/articles/read/connecting-the-military-microgrid-dots ("[T]hree microgrids, at the hospital at Naval Base San Diego, a data center at Naval Base Coronado, and at Naval Base Point Loma, are now equipped with the on-site generation, solar power, energy storage, and grid controls they need.").

215. Sec'y of the Air Force Pub. Affairs, *Beale Selected for Resilient Energy Demonstration Initiative*, Air Force, Apr. 28, 2016, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/745020/beale-selected-for-resilient-energy-demonstration-initiative.aspx. Relatedly, the Air Force's Office of Energy Assurance ("AF-OEA") was recently designated as the central management office to "develop, implement, and oversee an integrated facility energy portfolio, including privately-financed, large-scale renewable and alternative energy projects . . . ." Memorandum from Deborah Lee James, Sec'y of the Air Force, and Mark A. Welsh III, Gen. of the Air Force, Establishment of the Air Force Office of Energy Assurance (Feb. 23, 2016). The AF-OEA will also partner with the Army's Office of Energy Initiatives and the Navy's Renewable Energy Program Office. *Id.*

216. *Id.*

217. For a discussion of "military exceptionalism," see, e.g., Acevedo, *supra* note 23, at 353 ("Inevitably, such broad and blatant military exceptionalism further perpetuated the notion that military readiness and environmental protectionism do not (and arguably cannot) coexist in the U.S."); Hope Babcock, *National Security and Environmental Laws: A Clear and Present Danger?*, 25 Va. Envt'l. L.J. 105, 146 (2007) ("The combination of an unhappy armed forces and a 'self-declared,' politically compelling 'war against terror' has turned out to be lethal, not only for civil liberties but also for the laws and policies that protect the environment and the public's access to critical information about environmental risks."); Light, *supra* note 23, at 880–81 ("The military is largely exempt from environmental laws and regulations covering such broad areas as habitat conservation and information disclosure rules concerning toxic chemicals—at least when those laws conflict with the military's mission to protect national security.").

the rubric of "national security."[218] Generally speaking, DoD contracting officers, civil engineers, attorneys, and the like must all work within the federal regulatory regime in order to get things done. Unless there is a national emergency,[219] the DoD operates very much like any other federal agency when it comes to following regulations. Because the DoD is required to navigate the practical and regulatory challenges that invariably arise in the course of tackling an ambitious project like energy security, this section attempts to highlight and discuss those issues in greater detail.

A. Regulatory Issues

The DoD will encounter two broad categories of *federal* regulations affecting its acquisition of microgrids: procurement and environmental regulations. Both categories will be discussed here in turn.

1. Procurement

The DoD's procurement of renewable energy is usually accomplished using one of several statutory authorities. The first of these authorities is the power purchase agreement ("PPA"), which is authorized specifically for the DoD in 10 U.S.C. § 2922a (2012) (formerly 10 U.S.C. § 2394). This only-recently-used[220] statutory provision allows the Secretary of a military department to enter into contracts for a period of up to 30 years "for the provision and operation of *energy production facilities* on real property under the Secretary's jurisdiction or on private property and the purchase of energy produced from such facilities."[221] When Congress enacted this statute, "[t]he use of the authority . . . [was] not intended to enable a military department to compete with a public or private utility. It [was] intended to permit the exploration of a wide range of co-generation possibilities so that the conservation of scarce resources may be maximized."[222] The General Services Administration ("GSA") procures utility services for other federal agencies in accordance with 40 U.S.C. § 501 and FAR Part 41.[223] Unlike the DoD's PPAs,[224] however, the GSA is only allowed to enter into PPAs for periods of up to 10 years.[225]

Using a PPA, the DoD can contract to purchase all or a portion of the electricity generated within a microgrid for a definite term.[226] Under the PPA model, a third-party developer would have the option of either owning or leasing the

218. Although the Competition in Contracting Act ("CICA") allows for sole source acquisitions in cases of "national emergency," the DoD must still operate within the requirements of the statute and its corresponding regulations. *See* 10 U.S.C. § 2304(c)(3)-(6) (2012) ("The head of an agency may use procedures other than competitive procedures only when . . . it is necessary to award the contract to a particular source or sources in order [ ] to maintain a facility, producer, manufacturer, or other supplier available for furnishing property or services in case of a national emergency . . ." or "the disclosure of the agency's needs would compromise the national security . . . ."); *see also* 48 C.F.R. § 6.302-6 (a)(2) (2016) ("Full and open competition need not be provided for when the disclosure of the agency's needs would compromise the national security unless the agency is permitted to limit the number of sources from which it solicits bids or proposals."). Other "national security" exceptions, exemptions, or waivers in the Federal Acquisition Regulation ("FAR") typically require an agency head to approve the action in writing and notify either a higher authority or Congress. *See, e.g.*, 48 C.F.R. § 9.108-4 (2016) ("Any agency head may waive the prohibition in subsection 9.108-2 and the requirement of subsection 9.108-3 for a specific contract if the agency head determines in writing that the waiver is required in the interest of national security, documents the determination, and reports it to the Congress."); 48 C.F.R. § 22.1305(b) (2016) ("The head of the agency may waive any requirement in this subpart when it is determined that the contract is essential to the national security, and that its award without complying with such requirements is necessary to the national security. Upon making such a determination, the head of the agency must notify the Deputy Assistant Secretary of Labor in writing within 30 days.").

219. Although the threat to the grid is a very serious one and the need to construct renewable energy sources and microgrids is urgent, the DoD would be hard-pressed to argue that it can avoid environmental regulatory requirements using a "national emergency"-type argument, absent, in most cases, Presidential or Secretarial-level approval. *See, e.g.*, Clean Water Act, 33 U.S.C. § 1323(a) (2012) ("The President may exempt any effluent source of any department, agency, or instrumentality in the executive branch from compliance with any such a requirement if he determines it to be in the paramount interest of the United States to do so; except that no exemption may be granted from the requirements of section 1316 or 1317 of this Act."); Clean Air Act, 42 U.S.C. § 7418(b) (2012) ("The President may exempt any emission source of any department, agency, or instrumentality in the executive branch from compliance with such a requirement if he determines it to be in the paramount interest of the United States to do so, except that no exemption may be granted from section 7411 . . . ."); Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. § 9620(j)(1) (2012) ("The President may issue such orders regarding response actions at any specified site or facility of the . . . [DoD] as may be necessary to protect the national security interests of the United States at that site or facility.").

220. The DoD did not use 10 U.S.C. § 2922a to purchase electricity for nearly thirty years. Amy S. Koch, *Rethinking State Regulatory Issues*, *in* Renewable Energy for Military Installations: 2014 Industry Review 6 (Am. Council on Renewable Energy ed., 2014). This acquisition vehicle was critical to DoD's funding of renewable energy projects since the significant capital costs would "generally be so high that appropriated funds alone [would be] insufficient and the project[s] would never get started." Scholtes, *supra* note 23, at 64.

221. 10 U.S.C. § 2922a(a) (2012) (emphasis added); *see also* Memorandum from John Conger, Acting Deputy Under Sec'y of Def. (Installations & Environment), to Assistant Sec'y of the Army (Installations, Energy & Env't) et al. (Nov. 9, 2012) [hereinafter Financing Energy Projects], http://www.acq.osd.mil/eie/Downloads/IE/Policy_Financing%20of%20Energy%20Projects%209Nov2012.pdf ("While the authority under section 2922a applies to a facility on DoD or private land, it does not apply to a facility on non-DoD Federal property."). Multiyear contracts for supplies are permitted if for the promotion of national security under 10 U.S.C. § 2306b(a).

222. H.R. Rep. No. 97-612, at 30 (1982), *reprinted in* 1982 U.S.C.C.A.N. 441, 470.

223. Light, *supra* note 23, at 926.

224. 10 U.S.C. § 2922a is an independent contracting authority not related to the *exemption* listed in 40 U.S.C. § 501(a)(2), the statute controlling the federal government's acquisition of public utility contracts. Section 501 states that the "Secretary of Defense may exempt the [DoD] from an action taken by the Administrator of General Services under this subchapter, unless the President directs otherwise, whenever the Secretary determines that an exemption is in the best interests of national security." However, section 2922a *is* specifically listed as an *exception* to 40 U.S.C. § 591, which typically prohibits federal agencies from purchasing "electricity in a manner inconsistent with state law governing the provisions of electric utility service . . . ." 40 U.S.C. § 591(a) (2012). The Secretary of a military department is therefore allowed to enter into contracts under section 2922a without having to comply with section 591(a). But, whether the DoD's selling counterparties would be excepted from subsection (a) (and, by extension, state law) is a different question depending on the contract vehicle used. *See* Koch, *supra* note 220, at 6–10 ("While the 'federal enclave' doctrine and the [section 591] exceptions may allow a DoD [*sic*] to except an installation from state utility franchise law requirements, it is not clear whether the exceptions would prevent an electricity seller from being subject to state utility regulation, although there is a logical reason why the exceptions and federal enclave doctrine should protect the electricity seller.").

225. Light, *supra* note 23, at 926 (citing 40 U.S.C. § 501 (2012)).

226. Siemens, Deep Dive on Microgrid Financing 8 (2014), https://w3.usa.siemens.com/smartgrid/us/en/microgrid/Documents/Siemens_Microgrid_Financing_eBook.pdf. Much of the financing for PPAs is dependent upon renewable energy tax credits, some of which were recently extended by Congress. *See* Cassandra Sweet, *Wind, Solar Companies Get Boost From Tax-*

microgrid, and could therefore be responsible for operating and maintaining the microgrid and its components for the duration of the PPA term.[227] One obvious advantage to this model is the risk-shifting involved: the third party, not the DoD, would be responsible if the microgrid failed to perform as promised.[228] Also, the terms of the PPA would likely require the DoD to pay for power only if it is actually generated, so if the microgrid fails to produce power, the DoD would pay nothing.[229] Moreover, in the likely event that microgrid technology changes in the course of the contract term and becomes more efficient, the third-party owner may be incentivized to upgrade the equipment to bring generating costs down. This all assumes, of course, that the DoD has no desire to own the microgrid or make the requisite investments itself.[230]

Because PPAs under section 2922a are limited only to energy *production* facilities, one might argue that a microgrid, by itself, does not fall within the statutory authorization. On the other hand, if a microgrid or distributed generation system is included as a performance specification in a contract for a renewable energy project, then this may be a way to piggy-back the technology onto future acquisitions of renewable energy sources.[231]

With regard to the performance of a PPA, because the return on investment for the third-party developer/financier is dependent upon the extended length of the contract, the inclusion in the contract of the standard FAR clause 52.249-2, Termination for Convenience of the Government ("Fixed Price"), will be an issue for the developer. Generally speaking, if a contract is terminated for convenience, this clause permits the reimbursement of costs related only for the work completed prior to the termination.[232] But, because the developer is relying upon the full stream of payments in order to realize its return in the long run, the parties will likely have to negotiate and agree to a modified clause that includes early termination fees for each year of the PPA's term.[233]

The next type of acquisition vehicle is the enhanced use lease ("EUL") (otherwise known as an "outgrant"), found in 10 U.S.C. § 2667. Under this authority, upon a determination by the Secretary of Defense[234] that such a lease will "promote the national defense or . . . be in the public interest," the DoD can lease its property for large-scale renewable energy projects.[235] The property leased will usually be excess property on an installation (with no public use),[236] and the DoD will receive in return either cash or in-kind consideration at fair market value.[237] The statute allows compensation in the form of, among other things, "construction of new facilities," "payment of utility services," "real property maintenance services," and "such other services relating to activities that will occur on the leased property as the Secretary concerned considers appropriate."[238] EULs have the potential to assist in the acquisition of microgrids because the installations using EULs can accept in-kind consideration in the form of energy security infrastructure improvements.[239] In an environment where installation commanders are experiencing declining operations and maintenance ("O&M") budgets, EULs can assist in offsetting those losses. One caveat, however, is that unless the Secretary (or his/her designee) determines that a EUL will "promote the national defense or be in the public interest," EULs are limited to terms of 5 years. But, unlike a PPA, which may or may not facilitate the acquisition of a microgrid by itself, EULs more explicitly contemplate the provision of "infrastructure improvements," like microgrids.[240]

The DoD's next potential acquisition tool is the energy savings performance contract ("ESPC").[241] ESPCs require no upfront capital from the DoD, but the energy service company ("ESCO") recovers its investment if the project generates cost savings over the life of the contract.[242] As such, the ESPC is cash-flow neutral in that "the amount of monthly energy savings is supposed to be at minimum equal to the

Credit Extension, Wall St. J., Dec. 15, 2015, http://www.wsj.com/articles/wind-solar-companies-get-boost-from-tax-credit-extension-1450311501.

227. *Id.*
228. *Id.*
229. *Id.*
230. After installation of the facility, the developer (not the DoD) owns, operates, and maintains the facility for the life of the contract. Third-party developers, unlike the DoD, can also take advantage of several tax benefits over the life of a project.
231. Yet, this will likely increase the price of the project, possibly making it cost-prohibitive.
232. *See* 48 C.F.R. § 52.249-2(f) (2015); *see also* Lucas Michelini, *Developers' Perspective of Certain Risks in Long-Term Energy Contracts With the U.S. Department of Defense*, *in* Renewable Energy for Military Installations: 2014 Industry Review 26 (Am. Council on Renewable Energy ed., 2014).
233. Michelini, *supra* note 232, at 26. Appropriate contract documentation consistent with FAR § 52.241-5, relating to providing the developer a revocable permit or license to enter the service location for any proper purpose under the contract is also required. *See* Financing Energy Projects, *supra* note 221, at 2. Real property outgrant documentation should also be consistent with DoDI 4165.70.
234. This authority is delegated to the Assistant Secretary of Defense for Energy, Installations, and Environment. This is for both sections 2922a and 2667.
235. *See* 10 U.S.C. § 2667(a) (2012); *see also* Light, *supra* note 23, at 927.
236. This often times helps developers avoid the "not in my backyard" ("NIMBY") response that some have to renewable energy projects. *See* Eliot Hinds & Ian Shavitz, *Creating Financeable Power Purchase Agreements for Military Renewable Energy Projects*, *in* Renewable Energy for Military Installations: 2014 Industry Review 21 (Am. Council on Renewable Energy ed., 2014); *see also* 40 U.S.C. § 102 (2012) (defining "excess property").
237. Light, *supra* note 23, at 927.
238. *See* 10 U.S.C. § 2667(b), (c).
239. Light, *supra* note 23, at 927 ("Installations using enhanced-use lease authority can accept in-kind consideration in the form of a discount on the DoD's electric bill or in the form of infrastructure that will enhance energy security.").
240. "For renewable energy projects that apply leasing authority found under 10 U.S.C. § 2667, the Military Department must demonstrate more than a mere passive activity. For production or procurement of facility energy to qualify as being consistent with the DoD energy performance goals and master plan DoD must do one of the following . . . . Structure the project to provide energy security for the installation by, e.g., *retaining the right to divert to the installation the energy produced by the project in times of emergency." See* Financing Energy Projects, *supra* note 221, at 4 (emphasis added).
241. "Energy savings performance contract' ("ESPC"), as authorized by 42 U.S.C. [§] 8287, means a contract (or task order) awarded to an energy service company ("ESCO") for up to 25 years that provides for the design, acquisition, financing, installation, testing, operation, and maintenance and repair of identified [energy conservation measures] at one or more locations." Press Release, The White House, Presidential Memorandum—Implementation of Energy Savings Projects and Performance-Based Contracting for Energy Savings § 6(b) (Dec. 2, 2011) [hereinafter Presidential Memorandum—Implementation of Energy Savings Projects and Performance-Based Contracting for Energy Savings], https://www.gpo.gov/fdsys/pkg/DCPD-201100920/pdf/DCPD-201100920.pdf. Like section 2922a PPAs, 10 U.S.C. § 591 does not preclude the DoD from entering into ESPCs. *See* Financing Energy Projects, *supra* note 221, at 3.
242. Siemens, *supra* note 226, at 9.

monthly payment needed to finance the improvements."[243] ESPC contracts by definition will contain terms that guarantee energy savings; thus, in the event the energy savings are less than those projected in the contract, the ESCO would require reimbursement to the DoD for the difference.[244] Another benefit to the DoD is that the ESCO incurs the cost of project execution, the acquisition and installation of the equipment, as well as the training of personnel to operate the equipment.[245] The contractor's payment is "contingent upon realizing a guaranteed stream of future savings, with excess savings, after the duration of the contract, accruing to the federal government."[246] ESPCs are competitive acquisitions, limited to terms of up to 25 years,[247] and are regulated under 10 C.F.R. Part 436, Subpart B and FAR Part 23.[248]

Similar to an ESPC is a utility energy service contract ("UESC"), which is the last acquisition vehicle contemplated in this section. With terms typically limited to a maximum of 10 years, UESCs involve the DoD entering into an agreement with a *utility* (as opposed to a ESCO), who agrees to pay upfront capital costs to implement selected energy conservation measures (which typically includes renewable energy sources).[249] During the term of the contract, the DoD "pays" for the cost of the UESC from the "avoided-costs-savings" that flow from the energy efficiency improvements.[250] UESCs can be implemented under any of three types of umbrella contracts,[251] including area-wide contracts ("AWCs"), basic ordering agreements ("BOAs"), and separate contracts.[252]

Depending on the project, the DoD may select one, or some combination of the acquisition vehicles discussed in this section. And, as long as the DoD's budgets remain constrained, third-party financing of renewable energy and microgrid projects will continue to be the norm (outside of the aforementioned grant funding). Apart from the acquisition issues and decisions presented, the DoD will also very likely face environmental planning issues when constructing a microgrid on an installation.

2. Environmental

The primary environmental regulation the DoD will encounter in its acquisition of microgrid and renewable technologies is the National Environmental Policy Act ("NEPA").[253] The NEPA process frequently occurs during the project acquisition stage, prior to the solicitation being released.[254] When the project is defined by a developer, however, the NEPA process may start after the solicitation of the project and then be completed prior to a final agency decision whether or not to approve the project.[255] NEPA's objective is to make sure the DoD component proposing a major project takes a "hard look" at the environmental consequences of a proposed action and to provide information on the environmental consequences to the public.[256]

The "heart of NEPA"[257] is contained within Section 102, which requires the DoD to prepare a "detailed statement" on "proposals for legislation and other major Federal actions significantly affecting the quality of the human environment."[258] This detailed statement, known as an environmental impact statement ("EIS"), must discuss all of the following: (1) the environmental impact of the proposed action; (2) any adverse environmental effects which cannot be avoided should the proposal be implemented; (3) alternatives to the proposed action; (4) the relationship between local short-term uses of man's environment and the maintenance and enhancement of long-term productivity; and (5) any irreversible and irretrievable commitments of resources which would be involved in the proposed action should it be implemented.[259] An EIS is not required for every proposed project, but, rather, only required for those "major" projects having a "significant" impact.[260]

A DoD component may be able to complete a less-burdensome "environmental assessment" ("EA"), rather than an EIS.[261] If the EA concludes that the proposed action is neither "major" nor "significant," then a "finding of no significant impact" ("FONSI") is appropriate, which would allow the agency to proceed with its project.[262] Outside of an EIS or an EA is a third category, called a "categorical exclusion"

243. *Id.*
244. *Id.*
245. Light, *supra* note 23, at 927 (citing Memorandum from Sherri Wasserman Goodman, Deputy Under Sec'y of Def., to Assistant Sec'y of the Army (Installations, Logistics & Env't) (Jan. 12, 1992), https://perma.cc/6QQD-UDDP).
246. *Id.* at 927–28. (quoting Presidential Memorandum—Implementation of Energy Savings Projects and Performance-Based Contracting for Energy Savings, *supra* note 241).
247. 42 U.S.C. § 8287 (2012) ("Each such contract may . . . be for a period not to exceed 25 years.").
248. *See, e.g.*, 48 C.F.R. § 23.205(a) (2016) ("Agencies should make maximum use of the authority provided in the National Energy Conservation Policy Act (42 U.S.C. § 8287) to use an energy-savings performance contract (ESPC), when life-cycle cost-effective, to reduce energy use and cost in the agency's facilities and operations.").
249. 10 U.S.C. § 2913 (2012); *see also* Light, *supra* note 23, at 928 (citing Fed. Energy Mgmt. Program, U.S. Dep't of Energy, DOE/GO-102009-2588, Utility Energy Services Contracts: Enabling Documents 9 (2013) [hereinafter Utility Energy Service Contracts], http://energy.gov/sites/prod/files/2013/10/f4/uesc_enabling_documents09.pdf).
250. Utility Energy Service Contracts, *supra* note 249, at 9; *see also* 10 U.S.C. § 2912 (2012) (allowing the Department of Defense to retain and reinvest energy savings—perhaps into microgrids).
251. Utility Energy Service Contracts, *supra* note 249, at 10.
252. *See* 48 C.F.R. § 41.205 (2016) (stating the FAR requirements for separate contracts).
253. "[A]lthough [NEPA] contains no express statutory exemption for military actions, NEPA's regulations create an 'emergency circumstances' exception." Light, *supra* note 23, at 890 (quoting 40 C.F.R. § 1506.11 (2016) (requiring federal agencies to consult with the White House Council on Environmental Quality when "emergency circumstances make it necessary to take an action with significant environmental impact without observing the provisions of these regulations.")).
254. *See* Fed. Energy Mgmt. Program, Large-Scale Renewable Energy Guide: Developing Renewable Energy Projects Larger Than 10 MWs at Federal Facilities 2–3 (2013) [hereinafter FEMP Guide], https://www1.eere.energy.gov/femp/pdfs/large-scalereguide.pdf.
255. *Id.*
256. *Id.* at 25.
257. Charles Gartland, *At War and Peace With the National Environmental Policy Act: When Political Questions and the Environment Collide*, 68 A.F. L. Rev. 27, 33 (2012).
258. 42 U.S.C. § 4332(C) (2012).
259. *Id.*; *see also* 40 C.F.R. § 1502.10 (2016) (providing a recommended format for drafting an EIS).
260. Gartland, *supra* note 257, at 35 (citing 42 U.S.C. § 4332(C) (2012)).
261. *Id.* (citing 40 C.F.R. §§ 1501.3-.4, 1508.9 (2016)).
262. *Id.* (citing 40 C.F.R. § 1508.13 (2016)).

("CATEX").[263] A CATEX is a "category of actions which do not individually or cumulatively have a significant effect on the human environment . . . and for which, therefore, neither an [EA] nor an [EIS] is required."[264]

In the context of renewable energy sources and microgrids, mere modifications to existing facilities or systems will likely be covered by a CATEX.[265] However, if new exterior constructions or facilities are involved, the agency will almost certainly need to complete an EA or EIS.[266] If, in process of planning for a large-scale renewable energy or microgrid project, the decision is made to prepare an EIS, "a vigorous cycle of investigation, public comment, document drafting, and revision occurs."[267]

The first step of this process involves determining the scope of issues to be addressed and identifying significant issues related to the proposed action.[268] After its decision to prepare an EIS, but before the scoping process, the agency should publish a notice of intent in the Federal Register.[269] Affected federal, state, and local agencies, Indian tribes, and other interested parties are invited to participate in the scoping process.[270] Information collected during this process will provide a "foundation from which to build an EIS."[271]

The "heart of an EIS" is its analysis of alternatives, including the proposed action.[272] This section of the EIS should "present the environmental impacts of the proposal and the alternatives in comparative form, thus sharply defining the issues and providing a clear basis for choice among options by the decisionmaker and the public."[273] A "no action" alternative—contemplating the *status quo*—and a preferred alternative (including an "environmentally preferred alternative") should be included in the alternatives analysis.[274] The analysis must also include appropriate mitigation measures for each reasonable alternative.[275]

The draft EIS ("DEIS") should, like the notice of intent, be published in the Federal Register.[276] The agency should assess and consider public comments, and if the comments reveal new information or raise substantial questions about the project, then, among other things, the agency may consider new alternatives, engage in additional studies, or alter the project.[277] No matter what decision the agency makes, however, public comments must be included in the final EIS ("FEIS").[278] The agency's final decision and rationale are contained within its "record of decision" ("ROD"), which is the action that triggers the possibility of a court challenge.[279]

Needless to say, a court challenge or, worse, an injunction, carries with it the risk of delaying a renewable energy or microgrid project for an extended period of time, perhaps even indefinitely. Therefore, DoD project planners and managers must do their best to engage the relevant stakeholders at every critical stage of the development process, and avoid any short-circuiting of NEPA's stringent requirements.

B. Practical Issues

The DoD's impediments to success in the area of energy security are not merely limited to statutory or regulatory challenges. Arguably more impactful than maneuvering the regulatory regime is the current political and technological barriers to energy security.

1. Political

When faced with the prospect of large scale, widespread use of decentralized distributed generation systems and microgrids, it is unlikely that the electric utility companies will go quietly into the night.[280] While this is more an issue of concern for private actors in states without competitive electricity markets, the utilities' lobbying efforts to avoid regulatory reform nonetheless affects the DoD by keeping new laws promoting distributed generation and microgrids from being enacted.[281] In the interest of protecting their monopolies over service areas granted by federal and state governments, utilities frequently view any customer generation of power as detrimental to their business model.[282]

Microgrids may lead to costs for utility companies, including increases "in the per-user share of capital costs for infrastructure maintenance; the need to provide standby power over normal capacity; system upgrades; the cost of safety and maintenance issues related to interconnection of the microgrids; and the cost of uncertainties in planning for infrastructure expansion or modification."[283] As a consequence, utility companies may avoid long-term contracts or capital upgrades if microgrids create too much uncertainty.[284]

263. *See* 40 C.F.R. §§ 1501.4(a)(2), 1508.4 (2016).
264. *Id.* § 1508.4.
265. See 32 C.F.R. § 775.6(e) (2016) for a list of circumstances where a CATEX is inappropriate.
266. "The NEPA compliance process adds time, uncertainty, and development expense to the development of a project. Private developers may or may not be willing or able to carry the costs of NEPA compliance work and at the same time be comfortable with unknowns that the process could introduce in terms of project design and function." FEMP Guide, *supra* note 254, at 40.
267. Gartland, *supra* note 257, at 36 (citations omitted).
268. *See* 40 C.F.R. § 1501.7 (2016).
269. *Id.* §§ 1501.7, 1507.6.
270. *Id.* § 1501.7(a)(1).
271. Gartland, *supra* note 257, at 36 (citations omitted).
272. 40 C.F.R. §1502.14 (2016).
273. *Id.*
274. *Id.*
275. *Id.*
276. *Id.* § 1503.1.
277. Gartland, *supra* note 257, at 36 (citing 40 C.F.R. § 1503.4 (2016)).
278. *Id.*
279. 40 C.F.R. § 1505.2 (2016) ("At the time of its decision or, if appropriate, its recommendation to Congress, each agency shall prepare a concise public record of decision."). "Unlike many other environmental statutes, NEPA itself contains no provision expressly accounting for judicial review of NEPA compliance." Gartland, *supra* note 257, at 36 n.68 (citing Robert Glicksman, *Chapter 3: Judicial Review Under NEPA*, *in* NEPA Law and Litigation § 3:1 (Thomson Reuters 2d ed., 2011)). "Courts have concluded, however, that the Administrative Procedure Act (APA) provides an avenue for suit." *Id.*
280. *See* Bronin, *supra* note 131, at 568 ("Utility companies, which tend to object to distributed generation—and, by extension—microgrids, have a significant impact on state law and on the financial feasibility of distributed generation projects.").
281. *Id.*
282. *Id.* ("[B]ecause microgrids involve exchanges of power and payment between multiple users . . . [s]uch exchanges could infringe on the monopolies enjoyed by utility companies, and so are vigorously opposed.").
283. *Id.* at 568–69.
284. *Id.* at 569.

One common issue that utility companies raise about microgrids is a concern about safety. They have complained that distributed generation systems may supply power to the utility-run central grid when the grid is down, therefore endangering repair workers who believe they are accessing de-energized lines.[285] But, the reality is that the technology exists to avoid these safety concerns, and those technologies have already been deployed for a significant period of time.[286] Moreover, national safety standards have already been created for "the interconnection of distributed generation to the central grid."[287]

The over 3000 electric utilities in the U.S. also have different rules and regulations concerning the interconnection of renewable energy projects.[288] Normally, "there is a state-mandated, minimal interconnection limit with a streamlined application process for systems under 1 MW in capacity."[289] But, if a project is "sized above the minimum allowable size, the load-serving utility can burden the project with departing load, standby, or other fixed charges, in addition to requirements for system impact studies or network upgrades."[290] Even worse, a utility may refuse to serve a user of a microgrid or distributed generation system by simply not allowing the user to connect to the grid.[291] Moreover, depending upon the state in which an installation is located, a microgrid may be subject to "exit fees" when the installation operates in islanded mode.[292]

2. Technological

As discussed in Part II, with each microgrid tested by the DoD so far, fossil fuel-powered generators were a necessary component of each system. This can be attributed in large part to the renewable energy sources used to power the microgrids and the fact that they only provide intermittent energy. Without the ability to store surplus renewable energy, those sources will be unable to provide power when it is needed—24 hours a day and 7 days a week—nor will those sources ever truly be able to compete with fossil fuels or nuclear power. "Energy storage carries electricity through time, just as transmission lines carry it through space—without it, electrical energy must be used at the instant it is generated."[293]

Advances in battery and other storage technologies, however, have the potential to change the game.[294] The present questions, though, are how fast will those advances come online, and will those advances be economical?[295] The somewhat-limited technologies that already exist are indeed becoming less expensive: "In 2007, the cost of large-format lithium-ion storage was about $900 per kilowatt-hour; that is down to about $380, and could drop below $200 by 2020."[296] But, relatively speaking, they are still expensive.

On the government research and development front, the DOE recently received $120 million to study an advanced battery system that incorporates nanotechnology.[297] It also took advantage of a $185 million appropriation by way of the American Recovery and Reinvestment Act of 2009, which provided matching funds for over a dozen energy storage pilot projects.[298] The total value of the projects is $772 million, with a potential aggregate capacity of 537 MW.[299] These projects are piloted primarily by one of DOE's "Energy Innovation Hubs"—in this case, the Joint Center for Energy Storage Research ("JCESR"), founded in 2012.[300] Led by the DOE's Argonne National Laboratory, "JCESR participants include government, academic, and industrial researchers from many disciplines."[301] JCESR's most promising development is the flow battery (used, too, in the aforementioned Miramar microgrid), which uses two liquid organic compounds that, when pumped into a reactor, flow adjacent to one another to generate a charge.[302] While not ready for

285. *See* Bronin, *supra* note 131, at 569.
286. *Id.*
287. *Id.* (citing Inst. of Elec. & Elecs. Eng'rs, Inc. (IEEE), 1547: IEEE Standard for Interconnecting Distributed Resources With Electric Power Systems (2003)).
288. Kevin Prince & Morgan Adam, *Siting and Technology Considerations*, *in* Renewable Energy for Military Installations: 2014 Industry Review 37 (Am. Council on Renewable Energy ed., 2014); *see also* Jeff St. John, *California Closes in on Smart Solar Inverter Rules*, GreenTech Media (Nov. 13, 2013), http://www.greentechmedia.com/articles/read/california-closes-in-on-smart-solar-inverter-rules ("[I]nverters need to be prevented from mistakenly sending electricity onto power lines that really have lost grid power—a capability known as 'anti-islanding.' Because national standards such as IEEE 1547 and ANSI/UL 1741 still prohibit this kind of functionality, SIWG is asking Underwriters Laboratory (UL) to push ahead with utility-specific amendments to allow testing to proceed in California, in advance of slower-developing changes for the national standards.").
289. *Id.*
290. *Id.*
291. Bronin, *supra* note 131, at 570 ("The Department of Energy has documented numerous examples of utilities charging unfair and outsized backup tariffs—supplemental, backup, and standby tariffs that distributed generators are required to pay to ensure access to the grid . . . [and sometimes] utilities . . . refuse to serve users of distributed generation, by refusing to connect them to the grid.").
292. Business Exec. for Nat'l Security Task Force on Microgrids, Power the Fight: Capturing Smart Microgrid Potential for DoD Installation Energy Security 44 (2012), http://nyssmartgrid.com/wp-content/uploads/Power-the-Fight-Microgrid-Report__Fall-2012.pdf.
293. Andrew H. Meyer, *Federal Regulatory Barriers to Grid-Deployed Energy Storage*, 39 Colum. J. Envtl. L. 479, 480–81 (2014).
294. Scott Nyquist, *How Energy Storage Could Change Everything About Renewables,* Fortune (Sept. 24, 2015, 2:36 PM), http://fortune.com/2015/09/24/future-renewable-energy-storage/.
295. Without sufficient storage capacity, renewable energy may hit a ceiling of 10% (by 2040) of the total global power supply. *Id.* Moreover, historically low gas prices have undermined the economic models supporting many renewable energy projects. *See, e.g.*, Diane Cardwell, *Renewable Energy Hits a Snag*, N.Y. Times, Oct. 11, 2015, http://www.nytimes.com/2015/10/12/business/energy-environment/renewable-energy-financing-hits-a-snag.html?_r=0 ("Low oil and gas prices have roiled the energy markets, and the specter of rising interest rates has rattled investors' confidence in the industry's returns.").
296. Nyquist, *supra* note 294.
297. Meyer, *supra* note 293, at 482 (citing Joint Ctr. for Energy Storage Research, DOE Energy Innovation Hub—Batteries and Energy Storage (2013), http://science.energy.gov/~/media/bes/pdf/hubs/JCESR_Fact_Sheet.pdf).
298. *Id.* at 483 (citing Elec. Advisory Comm., Energy Storage Activities in the United States Electricity Grid 3 (2011), http://www.sandia.gov/ess/docs/other/FINAL_DOE_Report-Storage_Activities_5-1-11.pdf).
299. *Id.*
300. *About JCESR*, Joint Ctr. for Energy Storage Research, http://www.jcesr.org/about/ (last visited May 30, 2016) (The mission "of these Hubs is to advance promising areas of energy science and engineering from the earliest stages of research to the point of commercialization.").
301. *Id.*
302. Tina Casey, *Flow Battery Vs. Tesla Battery Smackdown Looming*, CleanTechnica (June 21, 2015), http://cleantechnica.com/2015/06/21/flow-battery-vs-tesla-battery-smackdown-looming/.

widespread commercial use, flow batteries have the potential to surpass the performance and price of lithium-ion batteries, which are the current go-to for energy storage.[303]

Within the private sector, a number of venture-capital funded battery storage companies are being born, and large corporations, like Lockheed Martin, for example, are also entering into the energy storage market, realizing the massive upside potential of large-scale grid storage.[304] While the investment is indeed a promising sign, no cost-competitive battery storage "panacea" has yet emerged.

Furthermore, some have argued, even if cost-competitive battery storage technology existed, federal regulations "threaten to undermine the successful deployment of storage on the grid."[305] Since it is unclear how FERC would classify large-scale battery storage—as either power generation, transmission, distribution or load—there is a potential that "regulatory rules and categories tailored to the more rigid operation characteristics of legacy technologies" will hinder the business case for storage technology.[306] "Consequently, storage cannot compete on a level playing field with traditional resources in FERC-jurisdictional markets."[307]

In a promising development, however, this year FERC requested that operators of wholesale power markets "document any possible barriers to energy storage's participation in capacity, energy and ancillary service markets."[308] The impetus for the inquiry, an industry insider stated, was that FERC itself is now convinced that "barriers to participation of storage in the wholesale market could be leading to higher than necessary system costs."[309] FERC also recognized how battery storage has the potential to benefit the distribution grid by solar smoothing or peak shaving (both of which assist with intermittency issues), in addition to the possibility of participating in wholesale electricity markets.[310]

Energy storage is not the only potential technological barrier to the DoD being truly "off the grid." Some have advocated the use of nuclear technologies—small modular nuclear reactors—as a way to power microgrids.[311] SMRs are characterized by: "(1) an electrical generating capacity of less than 300 MW, (2) a primary system that is entirely or substantially fabricated within a factory, and (3) a primary system that can be transported by truck or rail to the plant site."[312] The Navy has used a similar small reactor technology on its submarines and aircraft carriers for decades.[313]

It is estimated that a 40 MW SMR plant could meet the electricity needs of about 90% of military installations.[314] But, much like large-scale battery storage systems, the technology is in its early stages. Moreover, skeptics of SMRs have noted the high costs of the technology, which may make it non-competitive in an increasingly commoditized electricity market.[315] Advocates of the technology, however, counter that SMRs have the potential to produce electricity at a low cost *and* quickly turn on and off, therefore allowing it to capture high electricity prices and avoid periods where the real-time price of electricity is low.[316]

Regardless of its current technological or cost limitations, SMR technology is likely here to stay. As mentioned in Part III, President Obama recently recognized the potential of SMRs in EO 13693 by including it in the definition of "clean energy."[317] A precursor to the EO was a memorandum of understanding ("MOU") between the DoD and DOE concerning their "cooperation in the development and pilot testing of emerging energy technologies," including microgrids and "small modular reactor nuclear energy."[318] And, in May of 2016, the Tennessee Valley Authority ("TVA") submitted the "first-ever permit application to the U.S. Nuclear Regula-

303. *See id.*

304. Peter Maloney, *Lockheed Martin Pushes Into Storage Market With Lithium, Flow Battery Offerings,* Util. Dive (Apr. 25, 2016), http://www.utilitydive.com/news/lockheed-martin-pushes-into-storage-market-with-lithium-flow-battery-offer/417966/ ("The company is pushing into the storage space on two fronts: the integration of lithium-ion systems and the commercialization of a new flow battery technology."); *see also* Jason Deign, *Storage Firms Attract More Long-Term Investors as Commercial Launches Multiply*, Energy Storage Update (Sept. 28, 2015), http://analysis.energystorageupdate.com/storage-firms-attract-more-long-term-investors-commercial-launches-multiply ("The U.S. energy storage market is seeing a shift in funding activity as venture capital and private equity funds start to fall in importance compared to institutional investors.").

305. Meyer, *supra* note 293, at 483.

306. *Id.* at 484.

307. *Id.*

308. Peter Maloney, *FERC Seeks Input From ISOs on Possible Market Barriers to Energy Storage*, Util.ity Dive (Apr. 19, 2016), http://www.utilitydive.com/news/ferc-seeks-input-from-isos-on-possible-market-barriers-to-energy-storage/417629 ("FERC has given energy storage providers until May 23 [2016] to comment on the reports it receives from the wholesale market operator.").

309. *Id.*

310. *Id.*

311. *See, e.g.*, Acevedo, *supra* note 23, at 375 ("Adopting a modified version of [the Navy's nuclear] technology at domestic military installations could largely combat the inherent limitations present with current renewable energy projects."); Stew Magnuson, *Advocates Tout Small Modular Nuclear Reactors for Military Installations*, Nat'l Def. Mag., June 2013, http://www.nationaldefensemagazine.org/archive/2013/June/Pages/AdvocatesToutSmallNuclearReactorsforMilitaryInstallations.aspx ("[T]he idea to revive nuclear power on military installations—and even in forward-operating bases in battle zones—is being promoted in some quarters. Advocates say the military could reduce its dependence on domestic local power grids, which are seen as vulnerable, and it could take fuel convoys off the roads overseas.").

312. Acevedo, *supra* note 23, at 376–77 (citations omitted). Current nuclear plants' base load is usually around 1000 MW or higher. *See Small Modular Reactors*, U.S. Dep't Energy, http://energy.gov/ne/nuclear-reactor-technologies/small-modular-nuclear-reactors (last visited May 30, 2016).

313. *Id.* at 378.

314. *Id.* at 375 (citing Marcus King et al., Feasibility of Nuclear Power on U.S. Military Installations 11 (2011), http://www.uxc.com/smr/Library%5CPotential%20Markets%20and%20Clients/2011%20-%20Feasibility%20of%20Nuclear%20Power%20on%20U.S.%20Military%20Installations.pdf).

315. Leonard Hyman & William Tilles, *Why Small Modular Nuclear Reactors Are Not the Next Biggest Thing*, OilPrice.com (Apr. 7, 2016, 1:55 PM), http://oilprice.com/Alternative-Energy/Nuclear-Power/Why-Small-Modular-Reactors-Are-Not-The-Next-Big-Thing.html ("Small modular reactors are neither a panacea nor likely to herald a nuclear power resurgence.").

316. Robert Fares, *3 Ways Small Modular Reactors Overcome Existing Barriers to Nuclear*, Sci. Am. (May 19, 2016), http://blogs.scientificamerican.com/plugged-in/3-ways-small-modular-reactors-overcome-existing-barriers-to-nuclear/ ("SMRs don't have the same scale issue that conventional nuclear plants do. Because they are smaller, they require less upfront investment (even if the cost per unit of energy produced is higher). Furthermore, they are less likely to produce a supply glut in the marketplace. These features combine to make SMRs a lot more appealing than conventional nuclear from a finance perspective.").

317. *See generally* 80 Fed. Reg. 15,871 (Mar. 9, 2015).

318. Memorandum of Understanding Between U.S. Dep't of Energy & U.S. Dep't of Defense: Concerning Cooperation in a Strategic Partnership to Enhance Energy Security 2 (2010), http://www.energy.gov/sites/prod/files/edg/media/Enhance-Energy-Security-MOU.pdf.

tory Commission ("NRC") for a [SMR]."[319] The NRC will review the application in the second quarter of NRC's 2016 Fiscal Year.[320] But, a fully-functioning SMR will likely be unavailable for use until at least 2024.[321]

IV. Onward and Upward: Recommendations Going Forward

Given the technological and regulatory limitations discussed so far, how can the DoD's goals of energy security and sustainability be met going forward? Where is reform needed and what can the DoD or the federal government do to facilitate the military's acquisition of microgrids? This section will discuss the path forward for the DoD by recommending three fairly modest, but specific, policy changes.

A. The DoD Must Identify Its Critical Facilities, Then, Where Feasible, Protect Them With Microgrids

In 2008, the DSC warned that the DoD had neglected to assess its own weaknesses and vulnerabilities by not identifying the critical facilities that needed secure and resilient electricity sources.[322] As a result, the DSC recommended that the DoD assess the relative risk of a power outage at each installation, identify the costs of options to satisfy power requirements, and make the business case to identify the options that bring risk to acceptable limits.[323] Additionally, the DSC recommended that the DoD should "develop a plan to 'island' critical missions from the grid by December 2009."[324] While the DoD failed to develop the plan to "island" critical missions by December 2009, it did partly comply with the DSC's risk assessment recommendation by releasing updated guidance to its installations in DoDI 4170.11, *Energy Management*, in late 2009, and then updating it again this year.[325] Yet, whether its installations are following through with that guidance is an entirely different matter.

A GAO report conducted last year found *some* good news: nineteen of the twenty installations inspectors visited or contacted "use backup generators to provide emergency power to certain facilities."[326] At the same time, however, as of "February 2015, none of the services had a complete inventory of [the industrial control systems] on their installations."[327] And, despite finding more widespread use of backup systems, it was unclear in GAO's report whether the backup systems used were being allocated to critical facilities where reliable power is needed, or whether the critical facilities' power needs were sufficiently met by the generators.

Based on the ambiguous data available and the fact the DoD has still not clearly met the DSC's recommendations, the DoD must *now* identify and prioritize its critical facilities—that is, those facilities upon which the Nation's security depends, as well as those crucial facilities directly supporting overseas contingency operations. Once those critical facilities have been identified, the DoD must *now*, at least, assess and determine (1) the average electricity needs for each facility, (2) the duration of time that each facility must operate on its own in the event of a catastrophic grid failure, and (3) whether the present electricity infrastructure currently meets the DoD's needs in light of its risk assessments.

For those critical facilities reliant exclusively on backup generators or without any redundant power supply, the DoD should implement a plan to integrate microgrids where it is feasible. As discussed in Part III, the DoD's test programs have already established that microgrids work, and that they provide a reliable capability to "island" critical facilities from the commercial grid. Additionally, if critical facilities are located on an installation where renewable energy sources are being developed, the DoD should consider including a microgrid in the project's planning and execution.

B. Energy Security Should Become a More Prominent Factor in Future Renewable Energy Acquisitions

In the post-World War II era, several military installations were dependent upon their own electric power plants because they were located in isolated locations beyond the reach of utility services.[328] Many of those installations operated these power plants late into the twentieth century.[329] But, the inefficiency of government owned and operated power plants and utility systems led to the DoD selling off plants and privatizing many of its utilities in the late 1990s and early 2000s.[330]

To be clear, the reforms suggested in this paper do not advocate a return to the old system of DoD owned and operated power plants. Especially in light of the DoD's limited electricity and energy security budget, third-party financing of renewable energy projects and microgrids presents the best business case for the DoD going forward. That said, the third-party financial arrangement presents a number of acquisition challenges beyond those highlighted in Part IV. For example, because of utilities privatization, the electrical infrastructure on many installations is now owned and operated by service providers under up-to 50-year contracts.[331]

319. Fares, *supra* note 316.
320. *Tennessee Valley Authority (TVA) Clinch River Site Early Site Permit (ESP) Application*, U.S. Nuclear Reg. Commission (Apr. 8, 2016), http://www.nrc.gov/reactors/advanced/clinch-river.html.
321. Rebecca Kern, *NRC Sets Variable Fees for Small, Modular Nuclear Reactors*, Bloomberg BNA (May 23, 2016), http://www.bna.com/nrc-sets-variable-n57982072842/.
322. Def. Sci. Bd., More Fight—Less Fuel, *supra* note 22, at 54 ("In many cases, installations have not distinguished between critical and non-critical loads when configuring backup power systems, leaving critical missions competing with non-essential loads for power.").
323. *Id.* at 58.
324. *Id.* at 67.
325. *See* DoDI 4170.11, *supra* note 119.
326. DOD Reporting GAO Report 2015, *supra* note 116, at 32.
327. *Id.* at 41.
328. Anthony Andrews, Cong. Research Serv., R41960, Federal Agency Authority to Contract for Electric Power and Renewable Energy Supply 6 (2011), http://nationalaglawcenter.org/wp-content/uploads/assets/crs/R41960.pdf.
329. *Id.*
330. *Id.*; *see also* Christopher J. Alutto, *Privatizing and Combining Electricity and Energy Conservation Requirements on Military Installations*, 30 Pub. Cont. L.J. 723, 728 (2001).
331. Business Exec. for Nat'l Security Task Force on Microgrids, *supra* note 292, at 43; *see also* 10 U.S.C. § 2688 (2012) ("The Secretary of Defense, or the designee of the Secretary, may authorize a contract for utility services . . .

These utilities privatization contracts were not written with microgrids in mind and, thus, may not include provisions that would permit modification of the installation's infrastructure.[332] Additionally, depending on the state where the installation is located and the acquisition vehicle(s) used, a microgrid *may* end up being classified as a public distribution utility, which could subject the developer and the microgrid to state regulatory proceedings and controls.[333] This problem could be exacerbated by the fact that, in many states, there is no consistent definition of "microgrid" under existing utility law.[334]

Putting these issues aside, the primary acquisition challenge faced by the DoD and third-party developers is the fact the current contracting regime does not provide enough flexibility to account for microgrids' price premium.[335] Although energy security is a stated objective for the DoD,[336] the current (unwritten) policy is that the cost of clean/renewable power should be equivalent to or less than that of conventional/traditional power on a life-cycle basis.[337] Because energy security infrastructure (like microgrids) can come at a higher cost (due to the capital investment in the automated switching hardware, control systems, and the logistics trail of maintaining, servicing, and operating the capability), some "renewable energy procurement[s] cannot be structured to simultaneously enhance on-base energy security."[338]

This year, in a report looking into defense infrastructure, the GAO found that there exists "no specific [DoD] requirement that identifies the level of energy security an installation should have" and, moreover, "energy security projects, such as a microgrid or power plant, cannot compete well against energy efficiency or renewable energy projects that have a return on investment."[339]

For some military bases, microgrids working in conjunction with renewable energy sources will provide energy savings and a net financial benefit.[340] A report conducted by Business Executives for National Security ("BENS") found that "approximately 25% of domestic installations can implement smart microgrid projects that would reduce annual energy costs"; but, in general, "these installations are located in States with higher-than-average current electricity prices . . . ."[341] The report continued that many "DoD installation microgrids will operate at a 'security premium' . . . ."[342] Echoing the DSC report issued years before, the BENS report concluded that a more complete assessment of the "economics of backup generation currently in use . . . , combined with consideration of the criticality of missions at specific bases, and the costs of alternative microgrid approaches, will all enable DoD to develop a specific policy regarding the idea of a security premium."[343]

The BENS report is indeed correct that the DoD must better assess risk and continue to evaluate the business case for microgrids and other emerging technologies. But, in addition to these steps, the DoD must adopt a more uniform acquisition approach towards energy security among the services. The policy should expressly allow consideration of the value of energy security, and the security tradeoffs that come from obtaining energy from the fragile electric grid or from conventional diesel-powered generators.[344] If energy security becomes a bigger factor in renewable energy procurements, this may promote a virtuous cycle whereby contractors innovate to include microgrids alongside large-scale renewable energy projects, thereby making future, more secure renewable energy generation more sought-after among the DoD community.

Additionally, in order to provide flexibility to developers, future competitive acquisitions should emphasize performance requirements for microgrids, as opposed to design or equipment requirements.[345] That said, an effective microgrid should have *five* performance characteristics: It should (1) integrate renewable and other distributed generation to power task-critical assets in times of emergency (the supply-side); (2) be shielded or firewalled from a cyber-attack; (3) have the capability to separate from

to have a term in excess of 10 years, but not to exceed 50 years, if the Secretary determines that a contract for a longer term will be cost effective.").

332. *See* Business Exec. for Nat'l Security Task Force on Microgrids, *supra* note 292, at 43.

333. *Id.* at 44. *But see* Koch, *supra* note 221, at 6–10; *supra* note 225 (discussing the exceptions to 40 U.S.C. § 591 (2012)).

334. Business Exec. for Nat'l Security Task Force on Microgrids, *supra* note 292, at 44.

335. *See* PEW Charitable Trusts, Power Surge: How the Department of Defense Leverages Private Resources to Enhance Energy Security and Save Money on U.S. Bases 32 (2014), http://www.pewtrusts.org/~/media/legacy/uploadedfiles/peg/publications/report/pewdodreport2013k-s10020314pdf.pdf ("In other words, there is a priority for energy security and clean energy, but no premium for them."); *see also* Business Exec. for Nat'l Security Task Force on Microgrids, *supra* note 292, at 24 ("Many DoD installation microgrids will operate at a 'security premium' that DoD needs to explore further.").

336. *See, e.g.*, 10 U.S.C. § 2924(3)(B) (2012) ("In selecting facility energy projects that will use renewable energy sources, pursuit of energy security means the installation will give favorable consideration to projects that provide power directly to a military facility or into the installation electrical distribution network. In such cases, projects should be prioritized to provide power for assets critical to mission essential requirements on the installation in the event of a disruption in the commercial grid."); *id.* § 2917(b) ("The development of a geothermal energy project . . . should include consideration of energy security in the design and development of the project."); NDAA for Fiscal Year 2012, Pub. L. No. 112-81, § 2822, 125 Stat. 1298, 1691 (2012) (". . . the Secretary of Defense shall establish a policy for military installations that includes . . . [f]avorable consideration for energy security in the design and development of energy projects on the military installation that will use renewable energy sources . . . .").

337. *See* Marr & Rickerson, *supra* note 97, at 7 ("DoD's increasingly sophisticated suite of renewable energy procurement options remains limited by requirements that the price of renewable electricity typically not exceed the price of conventional power.").

338. *Id.*; *see also* David Schill, Improving Energy Security at Air Force Installations 143 (Rand Corp. ed., 2015), http://www.rand.org/content/dam/rand/pubs/rgs_dissertations/RGSD300/RGSD361/RAND_RGSD361.pdf.

339. U.S. Gov't Accountability Office, GAO-16-164, Defense Infrastructure: Improvement Needed in Energy Reporting and Security Funding at Installations With Limited Connectivity 28 (2016) [hereinafter Infrastructure GAO Report 2016], http://www.gao.gov/assets/680/674801.pdf.

340. Business Exec. for Nat'l Security Task Force on Microgrids, *supra* note 292, at 8, 42.

341. *Id.* at 23.

342. *Id.* at 24.

343. *Id.* (explaining that microgrids and other security enhancements could be funded using this statute, which allows energy savings to be reinvested in "energy security measures"); *see also* 10 U.S.C. § 2912 (2012).

344. Marr & Rickerson, *supra* note 97, at 9.

345. *See* Business Exec. for Nat'l Security Task Force on Microgrids, *supra* note 292, at 34.

the commercial grid and sustain critical operations during prolonged power outages; (4) be able to sustain itself for periods measured in weeks or months, not days; and (5) manage installation of electrical power and consumption efficiency to reduce fossil fuel demand and cost (the demand-side).[346]

The Navy has been somewhat of a leader when it comes to incorporating energy security into its acquisitions and funding decisions. The Navy uses an "energy return on investment" calculation in order to "compare and prioritize potential energy investments."[347] One of its indicators is the capability an energy project has to "provide reliable energy to critical infrastructure."[348] By incorporating this factor, "energy security explicitly influences energy procurement decision making."[349] Although GAO discussed the Navy's method as "rudimentary," it is nonetheless a step in the right direction and could serve as a starting point for the other services.[350]

Another suggested approach is that the DoD establish tiers to analyze investments in energy security based on how critical a particular facility is.[351] Facilities "tiered" by the DoD as "critical" would be "allowed to procure renewable energy and energy security infrastructure at a higher price point than might otherwise be approved."[352] A PPA could be used to pay the conventional rate for renewable power, and then a fixed price could be used to separately pay for security services provided by the infrastructure.[353]

The aforementioned BENS report suggested establishing a "levelized" metric for microgrid projects, using a "Levelized Cost of Secure Energy ("LCOSE")."[354] This metric would consist of two parts: (1) a levelized cost of energy metric (which is already used in commercial practice today), in addition to including the "avoided life-cycle costs of any on-base back-up generation that a microgrid would render unnecessary"; and (2) "a life-cycle measure of electrical infrastructure upgrades needed to make an installation 'microgrid ready.'"[355] Using this metric, the DoD could better communicate its requirements "in terminology consistent with commercial practice (supporting a best-value selection of generation) and also isolating those factors that go into a 'security premium' at an individual installation."[356]

No matter how the "security premium" is considered—using one or more of the discussed approaches—the DoD must more prominently consider energy security (specifically, microgrids) in energy acquisitions going forward. Additionally, when acquiring microgrids (for critical facilities in particular), it should incorporate the five performance characteristics mentioned above.

C. *Adopt an All-of-the-Above Approach to Achieve Energy Security*

For the time being, renewable energy cannot alone provide sufficient power for a base's microgrid in the event of a catastrophic grid failure.[357] The vast majority of renewable energy sources are both variable and intermittent.[358] As a result, in the context of microgrids, renewable energy sources will need to be supplemented temporarily by older technologies, like diesel- or, preferably, natural gas-powered generators.

But, to the extent that emerging technologies continue to come online, the DoD should take advantage of them. This includes both energy storage,[359] such as, for example, the flow batteries used for the MCAS Miramar microgrid, as well as fuel cells and small modular reactors ("SMRs"). President Obama took a noble step in the right direction—towards the future—in EO 13693. As discussed above, SMRs and fuel cells are now classified as "alternative energy" sources, which can be used by federal agencies to meet the EO's total building electric and thermal energy goal (so long as the EO remains in effect).[360]

Congress should follow the President's lead and amend Section 203 of the Energy Policy Act of 2005,[361] as well as the 2007 NDAA to include "alternative energy" and its corresponding definition along with "renewable energy." This would allow the DoD to use, among other things, SMRs and fuel cells to meet its "clean energy" mandates, and could also promote the use of third-party financing vehicles to fund experimental projects on DoD lands going forward. Future clean energy mandates via EOs or statutes should, too, include these emerging technologies in the definition of "alternative energy." While the SMR "tail" certainly should not wag the microgrid "dog," a marriage between these two technologies has the potential to allow the DoD to truly go "off the grid" because SMRs do not have the intermittency

346. *See id.* at 53; *see also* SPIDERS Final Report, *supra* note 187.
347. Marr & Rickerson, *supra* note 97, at 7.
348. *Id.* at 7.
349. *Id.*
350. *See* Infrastructure GAO Report 2016, *supra* note 339, at 28 ("[A] Navy Headquarters official told [GAO] that energy security is considered a 'soft benefit,' or benefit that is not the central focus of the project, and that it is difficult to fund a large project based only on soft benefits.").
351. Marr & Rickerson, *supra* note 97, at 9.
352. *Id.*
353. *Id.*
354. Business Exec. for Nat'l Security Task Force on Microgrids, *supra* note 292, at 33.
355. *Id.*
356. *Id.*
357. Infrastructure GAO Report 2016, *supra* note 339, at 29 ("[O]fficials stated that because the amounts of intermittent renewable energy can vary significantly, it can cause fluctuations in power quality such as voltage and frequency on small or isolated electricity systems, which can damage equipment connected to them. These officials noted that the amount of electricity generated from solar and wind systems can vary significantly with ambient conditions such as cloud cover and wind speed.").
358. *Id.*; *see also* Acevedo, *supra* note 23, at 370 ("One of the oft-cited reasons that renewables do not dominate the energy market is that wind and solar energy, the two primary forms of renewable energy currently being used at military installations, are subject to severe intermittency limitations.").
359. Acevedo, *supra* note 23, at 371 ("[A]lthough we have infinite access to wind and solar power, the excess power generated must be almost immediately consumed because there is currently no way to economically store it. Nevertheless, as innovative battery technology develops, wind and solar energy may become more viable on a large scale."). Ms. Acevedo worries, however, that open access to a military installation's microgrid renders the system vulnerable to attack. *Id.* at 372. This author disagrees considering the heightened security measures on the vast majority of military installations, especially those facilities deemed "critical."
360. *See* 80 Fed. Reg. at 15,882.
361. *See* 42 U.S.C. § 15852 (2012); 10 U.S.C. § 2911 (2012).

issues that renewables do.[362] A remotely-situated military installation could even serve as the first experimental laboratory to test the fused technologies' (microgrid + SMR) feasibility for more widespread DoD use.

V. Conclusion

The ability of microgrids to save energy and facilitate its "clean" production greatly assists the DoD in attaining both its goals of energy security and sustainability. Similarly, because microgrid technology can help satisfy two political concerns—environmental protection and national security—its development and acquisition should be an objective for both sides of the aisle.[363] The intersection of the two political interests can also propel forward some of the reforms highlighted in this Article, thereby facilitating the DoD's acquisition of these necessary technologies in the years to come.

As stated in the introduction, over the course of our Nation's history, the DoD has been a catalyst for and a cultivator of technological innovation. Its growing use of microgrids and other related technologies is no different. If the DoD is indeed successful in securing its critical facilities by using innovative leveraging of third-party financing, it could serve as an ideal model for other federal agencies and perhaps even private institutions, as well.

362. Acevedo, *supra* note 23, at 376 ("[T]he time is ripe for on-land deployment of the Navy's nuclear reactor technology." SMRs also have the potential to be "installed underground, protecting against the vulnerabilities of a physical attack or natural disaster.").

363. *See* Light, *supra* note 23 ("The military has the potential to make an enormous impact on climate change policy, especially in its stimulation of strategies to reduce energy demand and encourage the use of renewables."). Although it may be impossible to completely kill both of these "birds" with one stone, there exists a real possibility to improve the DoD's response to both the threat of climate change and the threat of a grid failure with properly targeted regulatory reform, investment, and vision.