William Mitchell Law Review

Volume 40 | Issue 2 Article 9

2014

Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid

Roland L. Trope

Stephen J. Humes

BEFORE ROLLING BLACKOUTS BEGIN: BRIEFING BOARDS ON CYBER ATTACKS THAT TARGET AND DEGRADE THE GRID

> "[P]erfect protection [of the grid] is . . . not possible. There will be a successful attack at some point."[1]

> "The Electric Power grid makes an attractive target because it is the foundational critical infrastructure that underlies all others. A successful attack on the power grid causing a wide-area long-term outage would have significant national security . . . consequences."[2]

Roland L. Trope[†] and Stephen J. Humes[††]

1. MASS. INST. OF TECH., THE FUTURE OF THE ELECTRIC GRID 27 (2011), *available at* http://mitei.mit.edu/system/files/Electric_Grid_Full_Report.pdf.

2. David Koester & Michael Cohen, *Electric Power Grid Indications & Warning Tool*, MITRE CORP. 1 (2012), http://www.mitre.org/sites/default/files/pdf/12_3623.pdf.

† Roland L. Trope is a partner at Trope and Schramm LLP in its New York City office; an Adjunct Professor in the Department of Law, U.S. Military Academy at West Point; and a member of the ABA Task Force on Cybersecurity. His bio can be accessed at http://www.linkedin.com/in/tropelaw. He can be contacted at rltrope@tropelaw.com.

†† Stephen J. Humes is a partner at Holland & Knight LLP in its New York City office; a member of the ABA Section of Environment, Energy, & Resources; and an Adjunct Professor of Law at Quinnipiac University School of Law. His bio can be accessed at http://www.hklaw.com/Stephen-Humes/. He can be contacted at Steve.Humes@hklaw.com.

Disclaimer: The views expressed herein are solely those of the authors and have not been approved by, and should not be attributed to, the U.S. Military Academy at West Point, the Department of the Army, the U.S. Department of Defense, or the U.S. Government.

I. INTRODUCTION

Blackouts, even the briefest, shock, surprise, and confuse. They imprint their images on people's memories. Most residents in the Northeast United States and Ontario, Canada, remember where they were, what they were doing, and what it took to get their bearings during the great blackout of August 2003. When blackouts strike (they do not just "happen," they appear to "strike"), it is as if an anthill has been kicked or dug up; the orderly populace turns into a frenzy of "what's happening, what's going on?" The disruption does not spread—its reach is immediate and pervasive; it wraps a new universe around every inhabitant under the blackout.[3] Individuals struggle to orient themselves to having no power and to trying to figure out how long an outage they should prepare to endure. Blackouts, lasting minutes into hours, change lives and

3. A memorable description of a wartime blackout experience appeared in *The New Yorker* in 1942:

> We chose the top of a Fifth Avenue bus for the blackout. . . . [A]s we got aboard the conductor said to the driver, "Let's try to make the Pierre," . . . . The lights in the store windows were already out as we proceeded up the Avenue . . . . There was little traffic and the bus moved right along. It became obvious that we would overshoot the Pierre when we got to the Plaza . . . . People were sitting all around the fountain and Sherman looked larger than usual in the moonlight. . . . The lights in the buildings, in the Park, and on the street corners went out and about thirty seconds later the traffic lights did too. . . . This left only the red beacon on the top of the R.C.A. Building, and the moon. . . . The silence was the big surprise of the blackout, we thought, the darkness having been discounted.

Talk of the Town: Lights Out, NEW YORKER, May 9, 1942, at 12.

take lives.[4] Consider the following recent widespread outages and their effects on customers:

- In August 2003, approximately fifty million commercial and residential electric customers went without power for days in the Northeastern United States and Canada;[5] the outage started when "several key transmission lines in northern Ohio tripped due to contact with trees" and "initiated a cascading failure of 508 generating units at 265 power plants across eight states and a Canadian province";[6]

4. That blackouts "take lives" is not an exaggeration, and it happens because other critical infrastructure tend not to plan with sufficient imagination or seriousness for worst-case consequences of the causes and durations of blackouts. As recently observed during the blackouts caused by Hurricanes Katrina and Sandy, blackouts not only "take lives" but force doctors to choose who will receive life-saving electricity from backup power units, and who will be denied it and, in essence, dispatched to die—issues that will arise in blackouts following cyber attacks that disrupt the grid:

> When the floodwaters rose around New Orleans hospitals after Hurricane Katrina in 2005, doctors wondered whom to rescue first. Sick babies? Critically ill adults? The elderly?
>
> More than seven years later, as Hurricane Sandy hit New York City, Bellevue Hospital's basement filled with millions of gallons of floodwater from the East River. The physician heading the intensive care unit was told that most backup power was likely to fail. She would have six power outlets. Which of her 50 patients should get one?
>
> . . . .
>
> At Memorial Medical Center in New Orleans, after the levees failed, doctors chose to rescue babies, pregnant women and critically ill adults first, and they designated certain elderly and very sick patients to go last. The heat rose and the power failed. Roughly 20 of the remaining patients were medicated with morphine or a powerful sedative, or both, before they died. Doctors told me they hastened their deaths in desperation.

Sheri Fink, *Shelter From the Storms*, N.Y. TIMES, Oct. 28, 2013, at A27, *available at* 2013 WLNR 27044887.

5. Brian Wingfield, *Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months*, BLOOMBERG (Feb. 1, 2012, 11:00 PM), http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html.

6. GREGORY C. WILSHUSEN & DAVID C. TRIMBLE, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-507T, CYBERSECURITY: CHALLENGES IN SECURING THE MODERNIZED ELECTRICITY GRID 11 (2012); *see also* U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA: CAUSES AND RECOMMENDATIONS (2004), *available at* http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

- In late October 2012, 8,661,527 customers in New York, New Jersey, and Connecticut experienced outages in the weeks after arrival of the Hurricane Sandy-Nor'easter[7] and its accompanying storm surge of seawater;[8]
- In late July 2012, 680 million customers went without power across Northern India when "India's rickety power grid" failed "for the second time in two days."[9]

Such sustained blackouts expose and fragment our assumptions of normalcy and the dependable availability of reliable electricity. If voltage or frequency become unstable, or if spikes and drops reoccur, then large equipment and small devices short-out;

7. OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, HURRICANE SANDY-NOR'EASTER SITUATION REPORT #13, at 1 (2012), *available at* http://www.oe.netl.doe.gov/docs/SitRep13_Sandy-Nor'easter_120312_300PM.pdf.

8. James Barron, *Storm Barrels Through Region, Leaving Destructive Path*, N.Y. TIMES (Oct. 30, 2012), 2012 WLNR 22912767.

9. Amy Kazmin, *Power Restored Across Northern India,* FIN. TIMES (London), Aug. 1, 2012, at 1, *available at* LEXIS. The committee appointed by the government of India to investigate the causes of the outage found "no evidence of any cyber attack." REPORT OF THE ENQUIRY COMMITTEE ON GRID DISTURBANCE IN NORTHERN REGION ON 30TH JULY 2012 AND IN NORTHERN, EASTERN & NORTH-EASTERN REGION ON 31ST JULY 2012, at vi (2012) [hereinafter REPORT OF THE ENQUIRY COMMITTEE], *available at* http://www.powermin.nic.in/pdf/GRID_ENQ_REP_16_8_12.pdf.

Instead, the committee found that once loads and frequencies went out of balance, the operators could not bring the system back into balanced stability before the grid collapsed. For example, one of the contributing causes to the first day blackout (on July 30, 2012) was that

> after [Northern Region] got separated from [Western Region] due to tripping of 400 kV Bina-Gwalior line, the [Northern Region] loads were met through [Western Region-Eastern Region-Northern Region] route, which caused *power swing in the system. Since the center of swing was in the [Northern Region-Eastern Region] interface, the corresponding tie lines tripped, isolating the [Northern Regio] system from the rest of the NEW grid system.* The [Northern Region] grid system collapsed due to under frequency and further power swing within the region.

Id. (emphasis added).

Apparently, India's grid is so susceptible to peak usage overloads that when its most famous cricket player, Sachin Tendulkar, walks out to bat for India, it is reported that "[p]erhaps 400m watch on television, risking power surges to India's jerry-rigged grid, which end abruptly the moment Mr. Tendulkar gets out, as millions switch off." *Banyan: The Meaning of Sachin*, ECONOMIST, Oct. 19, 2013, at 48, *available at* 2013 WLNR 26138887.

expensive motherboards and processors go from being expensive tools to worthless debris. But limited duration blackouts have one still-point around which all expectations gravitate: the North American Bulk Power System (BPS) tends toward order, not chaos.[10] Customers tend to assume that the owners and operators of BPS companies will manage the crisis, inform customers of the cause and schedule for restoration of power, and restore power. Customers also tend to assume that once power is restored everything will go back to normal—reliable, full supply of power with no destructive spikes or drops, and no resumption of the hours or days experiencing the "dark ages."

What will the impact be, however, if instead of "back to normal," the populace discovers that some locations will remain blacked out not for days or weeks, but for months and possibly years? What if electricity service in a region existed only in widely separated "islands"? What if stabilizing and maintaining even those "islands of electricity" required scheduled "rolling outages" and rationing of electricity to the highest-priority customers (hospitals, first responders, telecommunications providers, etc.)? What if such prolonged, degraded, and unreliable supplies of electricity became an industry-wide "New Normal"? And what if the cause was not a one-off incident—a hurricane, earthquake,[11] storm-surge, or solar flare? What if instead the cause became identified only over weeks and months to be coordinated kinetic[12] cyber attacks? And what if these cyber attacks amounted to an industry-defined Severe Event, namely one so damaging that afterwards the electricity services

10. The apparent tendency toward order is an illusion, created by the moment-to-moment monitoring and adjustments of load balances and other factors that enable the large, interconnected BPS to remain stable instead of having its interconnectedness turn into a chaos of cascading blackouts.

11. In fact, as anyone who has lived through a major earthquake knows, strong earthquakes are never "one-off" events. There are aftershocks, some large enough to qualify as significant quakes by themselves, and the after-shocks often cause substantial, additional damage to structures and to the psyches and nerves of inhabitants who experience the tremors of each after-shock.

12. A "kinetic attack" is defined by the U.S. Department of Defense (DoD) as "one using weapons that rely on energy—blast, heat, and fragmentation, for example—to cause their damage. A non-kinetic attack might involve electronically disabling an enemy's computers and communication equipment." John Paradis, *Strategic Command Missions Rely on Space*, U.S. DEP'T DEF. (Sept 29, 2003), http://www.defense.gov/News/NewsArticle.aspx?ID=28408.

remained degraded for months or years. And finally, what if, in the meantime, the cyber attacks adapted to recovery efforts and continuously fed inaccurate supply-and-demand load data to operators of BPS generation, transmission, and distribution centers? What would the impact be on individuals, critical infrastructure, the nation's economy, and national security if these cyber attacks continued to cause recurrent disruptions and increased damage, made "trust deficits" a reoccurring burden on operators, and impressed on BPS companies and customers that the New Normal defined the scope of their plans, because no one knew with even remote certainty when the old normal might be restored? This is the most significant cybersecurity challenge that boards, management, and legal counsel of BPS companies need to confront. The subject of this essay is how to address that challenge responsibly.

We endeavor in this essay to assist BPS boards, management, and their legal counsel in addressing the cyber threats to the BPS and in making what appears to be an increasingly difficult choice between two paths to pursue in reducing the company's exposure to cyber risks. One path involves addressing risks identified by the executive branch in Executive Order No. 13636 (EO), adopting the Cybersecurity Framework (authorized by the EO) and focusing on improving company resilience to cyber attacks. The other path involves addressing risks identified by task forces (authorized by their regulator, the North American Electric Reliability Corporation (NERC[13])) and focusing on the task forces'

13. As explained in testimony by NERC's Executive Vice President to a congressional subcommittee:

> NERC's mission is to ensure the bulk power system in North America is reliable. To achieve this objective, NERC develops and enforces reliability standards; monitors the bulk power system; assesses and reports on future adequacy; evaluates owners, operators, and users for reliability preparedness; and educates, trains[,] and certifies industry personnel. NERC is a self-regulatory organization that relies on the diverse and collective expertise of industry participants. FERC certified NERC as the electric reliability organization (ERO) in July 2006.

The Cyber Threat to Control Systems: Stronger Regulations Are Necessary to Secure the Electric Grid: Hearing Before the Subcomm. on Emerging Threats, Cybersecurity, & Sci. & Tech. of the H. Comm. on Homeland Sec., 110th Cong. 39 (2007) (statement of David A. Whiteley, Executive Vice President, North American Electric Reliability Corporation).

recommendations for managing the consequences of a catastrophic cyber attack. The NERC task forces call this cyber attack a Severe Event because it results in such disruption and damage to the BPS that for months, if not years, the BPS operates at a level significantly below the pre-attack levels and requires rolling blackouts to stabilize the surviving "islands" of electric power.[14] Since it appears that many BPS company boards are not yet aware of the widening gap between the White House's and NERC's cybersecurity initiatives, we will devote much of this essay to explaining those initiatives and the choices and challenges that each presents to BPS company boards, management, and their legal counsel.

II. UPDATING BPS COMPANIES' WORST-CASE SCENARIO RISKS TO MATCH THE INCREASED SOPHISTICATION OF KINETIC CYBER ATTACKS

A. Reliance on the North American Bulk Power System Put at Risk by Cyber Threats

In North America, public access to a resilient and reliable supply of electric power—whenever needed—is our economic foundation; it is a critical constant supporting our quality of life and the quickening pace of digital technological innovations. As each wave of new digital communications technology gains widespread use and fosters, in turn, new prodigious data capture and search capabilities, the necessity of available, reliable, and resilient electric power whenever needed to operate or recharge devices is absolute.

NERC-sponsored cybersecurity initiatives include the recommendations found in the following documents, which are part of NERC's "Critical Infrastructure Roadmap." *See* N. AM. ELECTRIC RELIABILITY CORP., CYBER ATTACK TASK FORCE: FINAL REPORT 4–5 (2012) [hereinafter CATF REPORT], *available at* http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf; N. AM. ELECTRIC RELIABILITY CORP., HIGH-IMPACT, LOW-FREQUENCY EVENT RISK TO THE NORTH AMERICAN BULK POWER SYSTEM (2010) [hereinafter HILF REPORT], *available at* http://www.nerc.com/pa/ci/resources/documents/hilf_report.pdf; N. AM. ELECTRIC RELIABILITY CORP., SEVERE IMPACT RESILIENCE: CONSIDERATIONS AND RECOMMENDATIONS (2012) [hereinafter SIRTF REPORT], *available at* http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

14. *See* SIRTF REPORT, *supra* note 13, at 2–3.

When employees arrive at work, they assume that when they try to illuminate their office space, power up their computers, and recharge their battery-operated phones and portable computing devices (pads, tablets, phablets), the power will flow without interruption, without destructive surges or plummets, and will keep doing so without requiring their attention, oversight, or intervention. For decades, when boards of directors met to oversee management's handling of risks to an enterprise, the board members seldom, if ever, asked:

- What is the risk that our company's need for electricity will be met in the next quarter?
- Do we have contingency plans in place to ensure that, in the event that a coordinated cyber attack on the BPS causes a regional outage that lasts for weeks or months, our company can procure the electricity needed to continue operation and production without disruption?

Those questions might once have been met by management and board members with incredulity. They would have seemed far-fetched, the kind of wrong question that humans ask the computer "Deep Thought" (in *A Hitchhiker's Guide to the Galaxy*) and to which they receive the incomprehensible answer "forty-two."[15] Now, however, such questions are pertinent and timely. Boards and management need to adjust their risk management in order to address not far-fetched, but worst-case scenario questions relating to kinetic cyber attacks that now have immediate relevance.

By now, the boards of many companies have come to view the security of corporate intellectual property and business information against the risks of cyber intrusions and cyber attacks as a top priority.[16] Nevertheless, cybersecurity risk remains "a difficult and intimidating topic for corporate boards to consider."[17] The main reasons are well known:

- Each year the learning curve for cybersecurity becomes longer, steeper, and tougher to climb.

15. *See* DOUGLAS ADAMS, THE HITCHHIKER'S GUIDE TO THE GALAXY 151–53 (1979).

16. Paul Taylor, *Security Tops Boardroom Agendas*, FIN. TIMES (London) (Apr. 24, 2012, 11:56 PM), http://www.ft.com/intl/cms/s/0/47b3bfec-8978-11e1-85b6-00144feab49a.html#axzz2tDDhVp5D.

17. David A. Katz & Laura A. McIntosh, *Corporate Governance Update: Cybersecurity Risks and the Board of Directors*, 248 N.Y. L.J. 5, 5 (2012).

- The ability of cyber adversaries to probe, find vulnerabilities, and launch sophisticated and stealthy attacks against company networks continues to outpace the ability of target companies to defend, detect, and thwart such attacks.
- And, unlike other corporate crises, boards and management must be ready to address severe cyber incidents with response and recovery plans that activate upon discovery of an intrusion and with little or no time for deliberation.[18]

These challenges become formidable and daunting when, instead of non-kinetic attacks on information systems, a board and management must address the risks of *kinetic* cyber attacks that target the control systems and operations run by a critical infrastructure company. The potential consequences for the company's reputation, finances, and survival—and for third parties that depend on its services—become prodigiously far reaching for a board and management responsible for a company that operates part of the BPS. As pointed out in a National Academy of Sciences study released in November 2012, "The electric power delivery system that carries electricity from large central generators to customers could be severely damaged by a small number of well-informed attackers."[19] Such an attack "could deny large regions of the country access to bulk system power for weeks or even months."[20] Soon after taking office, Energy Secretary Ernest Moniz made clear in August 2013 that the executive branch views the "threat of a cyber attack shutting down the U.S. electric grid" as its most serious concern.[21]

B. The Salient Questions for a BPS Board and Management When Confronted by Risks of Kinetic Cyber Attacks

BPS owners and operators, when addressing the risks of kinetic cyber attacks against their companies, will probably continue to do

18. *See id.*

19. NAT'L RESEARCH COUNCIL, TERRORISM AND THE ELECTRIC POWER DELIVERY SYSTEM 1 (2012), *available at* http://www.wiresgroup.com/docs/WPF_Terrorism%20and%20The%20Electric%20Power%20Delivery%20System.pdf.

20. *Id.*

21. Paul Bedard, *Energy Secretary: Cyber Attack, Not EMP, Is Biggest Threat to Electric Grid*, WASH. EXAMINER (Aug. 1, 2013), http://washingtonexaminer.com/energy-secretary-cyber-attack-not-emp-is-biggest-threat-to-electric-grid/article/2533756.

as they have customarily done: attempt to assess risks and endeavor to manage them effectively and responsibly. But these owners and operators appear to sense that with the emergence of credible threats of kinetic cyber attacks against BPS company operations, the stakes have become much higher and the time frames within which they and their boards of directors must take decisive action have shrunk from weeks to hours to minutes. As two corporate commentators recently observed:

> One potential difference between cybersecurity crises and other corporate crises is that both internal and external aspects of crisis management with respect to a cyber incident must begin within hours rather than days, in order to be as effective as possible. Directors should expect management to be prepared to respond very quickly to any cyber attack.[22]

As a result, when the federal government identifies a cyber threat to national security whose targets include companies that operate the nation's critical infrastructure, boards of directors of the targeted companies (including BPS companies) may ask some preliminary, cautionary questions of senior management in order to ensure they are assessing the risks and adequately addressing them. The questions may take many forms, but ultimately boards of directors will probably be seeking answers to the following:

- How seriously should our company take the government's declaration of this cyber threat?
- If the cyber threat poses a serious risk to our company, is the main risk to our company's business information systems or to its operation and control systems?
- If the main risk of the cyber threat is to our company's operation and control systems, how comprehensive should our company's preparations be?
- What priority and urgency should our company give to completing those preparations?
- In the absence of a uniform federal or state standard for critical infrastructure cybersecurity, by what standard will our response to this cyber threat ultimately be judged?

In preparation for such discussions, the board may ask counsel to provide an analysis that helps management understand the

22. Katz & McIntosh, *supra* note 17, at 5.

cybersecurity risks to the company and the extent to which the company is responsible for addressing risks that originate offshore in planned kinetic cyber attacks that target critical infrastructure companies in the United States. Although there is a growing consensus on the magnitude of the threats and risks of kinetic cyber attacks against critical infrastructure companies, there is a remarkable lack of consensus and considerable confusion regarding who is responsible for addressing such risks and threats—the federal government or private industry. We address that issue in the next section.

III. WHO HAS THE RESPONSIBILITY FOR ADDRESSING RISKS OF KINETIC CYBER ATTACKS AGAINST BPS COMPANIES?

BPS company boards and management face a narrowing window of time in which to confront and manage risks from kinetic cyber attacks. The risks are increasing as the result of three converging phenomena:

First, the increasing interdependence of rapidly growing, high-tech industries (such as cloud computing) and the immense quantities of electric power they consume, dissipate as heat, and require for cooling.[23]

23. Cloud computing is precariously dependent on a reliable supply of electric power (since any unevenness in that supply can damage the equipment), and the electricity cost has become the chief operating expense. For example, the enormous server farms that support cloud computing and big data analyses depend on reliable supplies of prodigious quantities of electric power. For each kilowatt-hour of power needed to operate a cloud computing facility's acres of servers, those servers dissipate an equal amount of heat requiring an additional kilowatt-hour of power to cool the air surrounding the servers. As researchers have explained:

> Cloud computing is hot, literally. Electricity consumed by computers and other IT equipment has been skyrocketing in recent years, and has become a substantial part of the global energy market. . . . Energy efficiency is . . . important to reduce operational costs . . . [because] cooling cost is significant in centralized data centers due to the power density.

JIE LIU ET AL., THE DATA FURNACE: HEATING UP WITH CLOUD COMPUTING 1–2 (2011), *available at* http://research.microsoft.com/pubs/150265/heating.pdf. The dissipated heat is so high that researchers propose that data centers be used as "data furnaces" and be the primary heat sources for offices and homes. *Id.* at 2.

Second, the increasing fragility of electric power grids (such as the BPS) as equipment ages, as cyber vulnerabilities proliferate (and remain uncorrected), and as "smarter" devices with software flaws are deployed that create two-way communication channels and nodes that provide adversaries vulnerable points and attack vectors.[24]

Third, the growing risk that adversaries are now capable of launching coordinated kinetic cyber attacks capable of damaging the BPS so severely and extensively that service might not be restored to pre-event levels for months, if not years.[25]

Boards of directors and management of critical infrastructure (all of which are dependent upon, and interconnected with, the BPS) will therefore need to determine who has the responsibilities for addressing such risks and making the preparations to cope with post-attack recovery. Do those responsibilities remain in the hands of the federal government (as it would in the event of a tangible, kinetic attack against the tangible assets in the U.S. homeland), or has a significant part of those responsibilities been relegated to private industry?

A. The Scope of Federal Government Cyber Responsibility and Authority Is Unclear

lf a foreign-based or foreign-planned kinetic or non-kinetic attack is launched against the U.S. homeland and involves an assault across the U.S. border (or from within the U.S. homeland using chemical, biological, radiological, or nuclear weapons as a terrorist attack) and targets critical infrastructure, the attack immediately implicates national security and is addressed by the responsible agencies accordingly. The federal government has clear and full responsibility for intelligence, defense (including preemptive strikes), interdiction, and counter-strikes. Federal government responsibility for national defense concerning tangible, visible weapon attacks against tangible, visible targets is clear and familiar.[26]

24. *See infra* Part IV.B–IV.D (discussing the vulnerabilities introduced by "smart grid" technologies).

25. *See infra* Part IV.D (discussing the emerging cyber threats to the BPS).

26. It extends also to foreign terrorist attacks launched within the United States, such as the attacks that occurred in 1993 and 2001. Note also that at least as

But what happens when the foreign attacker launches invisible, intangible sorties of electrons through the Internet, injects intangible malware invisibly through a vulnerable wireless connection, or hacks into a two-way communication "smart" device node and eventually succeeds in making a kinetic attack? Even though the result might be long-term damage to operational equipment and reduces, for months, the service capabilities of a critical infrastructure company (such as power plants or the transmission system), it is unclear whether the federal government or private industry has primary responsibility for addressing the incident. In other words, what if, instead of a few trees touching power lines in Ohio and tripping off the regional power grid in the Northeast, a rogue foreign actor infiltrates the power grid and trips off the same cascading outages? The attack poses an immediate and substantial danger to the nation. For that reason, it too implicates national security; but, efforts to respond to such attacks on the defense and information technology sectors of critical infrastructure (and they have occurred) have not been well organized, coherent, vigorous, or particularly effective. Reportedly, the targeted companies (e.g., Lockheed Martin and Silicon Valley companies such as Google), who are among the nation's largest and developers of its most sophisticated technologies, experienced severe cyber attacks.[27] Chief among the reasons for the lamentable

early as 1998, the DoD conducted exercises and drills involving simulated armed assault on offices within the Pentagon, including one on May 30, 1998 called "Cloudy Office" that was part of an "effort to improve the nation's overall ability to respond to incidents involving nuclear, biological or chemical agents." Alicia K. Borlik, *DoD Drill Tests Response to Terrorist Attack*, U.S. DEP'T DEF. (June 9, 1998), http://www.defense.gov/News/NewsArticle.aspx?ID=43179. However, it is unclear from the DoD press release which agency had ultimate authority over the command and control of the response to the simulated lethal nerve agent attack and taking of hostages. *See id.*

27. Reports of cyber attacks on Lockheed Martin appeared in 2011 and 2012. *See* Dara Kerr, *Cyberattacks Against Lockheed Have 'Increased Dramatically,'* CNET (Nov. 12, 2012, 8:05 PM), http://news.cnet.com/8301-1009_3-57548766-83/cyberattacks-against-lockheed-have-increased-dramatically/; Mathew J. Schwartz, *Lockheed Martin Suffers Massive Cyberattack*, INFO. WK. (May 30, 2011, 7:58 PM), http://www.informationweek.com/government/security/lockheed-martin-suffers-massive-cyberatt/229700151. Although Lockheed Martin claimed that these later attacks did not access sensitive information, an earlier series of attacks against it in 2009 were apparently quite successful in exfiltrating data related to the design of the Joint Strike Fighter: "[W]hile the spies were able to download sizable amounts

and ineffectual response against the attackers would seem to be that the intangible and invisible nature of the attacks and the advanced technology used to carry them out have proceeded without an immediate determination of responsibility for addressing them.[28]

of data related to the jet-fighter, they weren't able to access the most sensitive material, which is stored on computers not connected to the Internet." Siobhan Gorman, August Cole, & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, WALL ST. J., Apr. 21, 2009, at A1, *available at* LEXIS.

Accounts of the attacks on Google and other Silicon Valley tech companies appeared, for example, in January 2010:

> Those attacks, which Google said took place last week, were directed at some 34 companies or entities, most of them in Silicon Valley California . . . . The attackers may have succeeded in penetrating elaborate computer security systems and obtaining crucial corporate data and software source codes, although Google said it did not itself suffer losses of that kind.

Andrew Jacobs & Miguel Helft, *Google May End Venture in China Over Censorship*, N.Y. TIMES, Jan. 13, 2010, at A1, *available at* 2010 WLNR 676831*; see* Cade Metz, *Cyberattack Lifted Google Password System Code, Says Report*, REGISTER (Apr. 20, 2010), http://www.theregister.co.uk/2010/04/20/reports_says_cyberattack_on_google_lifted_code_for_password_system/. None of these accounts suggest a vigorous or organized response by the U.S. Government or by any of the companies attacked beyond attempting to halt the attack after its detection. The reports do not disclose how long the attacks may have been proceeding before their detection and whether they continued after detection. Although these uncertainties may be deliberate, they also leave unclear what, if any, outside agencies may have assisted the attacked companies. In the case of Lockheed Martin, of course, the company would have reported the breach to its customer, the DoD. Such reports are now mandatory under recent DoD-issued regulations applicable to its contractors and subcontractors at every tier.

28. Moreover, with the emergence of the "Internet of things" with sensors, RFID-chips, and other means of communicating to the Internet attached to every quotidian object, the vulnerability to cyber attacks will escalate substantially, as noted in a recent *Financial Times* essay:

> [W]e are about to undergo a technological shift that will bring the connectivity of the internet into every aspect of life. Marketers call it the "internet of things," where everything, from shoes to pacemakers, will have an internet connection—a tenfold increase in the number of connected devices is expected by 2020.
>
> The damage that it will be possible to inflict through cybercrime, warfare or terrorism will increase exponentially. No longer limited to cyberspace, hackers will be able to overload a power grid or derail a train if desired.

Bede McCarthy, *Secrecy Hampers Battle for Web*, FIN. TIMES (London), June 7, 2013,

It is doubtful that federal government officials believe that they are responsible for addressing the risks of kinetic cyber attacks against critical infrastructure companies because there is so much uncertainty expressed concerning the limited government authority to respond to the threats of such attacks. The efforts to enact comprehensive cybersecurity legislation evidence a belief in Congress that, without such legislation, the federal government lacks the authority to respond to such threats or to require private industry to improve cybersecurity in order to mitigate or thwart the effectiveness of kinetic cyber threats. Moreover, we have found no evidence to suggest that BPS and other critical infrastructure companies have a clear understanding of where the government's limited responsibility ends and where private industry's responsibility begins.

When the World Trade Center collapsed after a tangible attack—although local municipal and state fire, police, and medical service personnel had responsibility for the "first response" on the scene—the federal government was responsible for addressing future similar attacks and for pursuing those responsible for planning and carrying out the attack.[29] But if a major segment of the Eastern Interconnect of the BPS collapsed after a cyber attack (and its service could not be fully restored to pre-attack levels because transformers and other equipment with

at 1, *available at* LEXIS.

29. With respect to the 9/11 attack on the Pentagon, a subsequent study of the response on the scene observed:

> The initial response to the Pentagon attack was performed by the fire and emergency units from the Arlington County Fire Department (ACFD), the Fort Myer Fire Department (a U.S. Army Base located adjacent to the Pentagon), and the Metropolitan Airport Authority Fire Unit at Ronald Reagan National Airport . . . [all of which] responded without any state or Federal intervention or control.
>
> The Federal mobilization of resources for the response was governed by the structure and process defined in the Federal Response Plan (FRP). . . . State and local authorities retained the primary authority to respond to the consequences of terrorism, and FEMA was assigned responsibility for coordinating federal assistance as required.

GEORGE WASH. UNIV. INST. FOR CRISIS, DISASTER, & RISK MGMT., OBSERVING AND DOCUMENTING THE INTER-ORGANIZATIONAL RESPONSE TO THE SEPTEMBER 11TH ATTACK ON THE PENTAGON § 4.1 (2002), *available at* http://www.gwu.edu/~icdrm/publications/nsf911/response.html.

long lead time were damaged),[30] there would be considerable dispute afterwards as to who was responsible for failing to prevent it (the federal government or the BPS operators and owners) and who was responsible for managing the long-term recovery. Quite simply, who is responsible for defending against a cyber attack against the BPS or for identifying its origin and the adversary who planned and carried it out? Evidence of the uncertain and limited role to date by the federal government appears in a 2011 report by researchers for McAfee and the Center for Strategic & International Studies in their second annual critical infrastructure protection report. The researchers observed: "How are governments responding to the vulnerability of their core civilian infrastructures? In general, they continue to play an ambiguous role in cybersecurity—sometimes helping the private sector, sometimes ignoring it."[31]

B. The Scope of Private Industry Cyber Responsibility and Authority Is Unclear

If responsibility for addressing risks of kinetic cyber attacks against critical infrastructure ultimately rests with private industry (as it appears to), the allocation has not been made by any clear decision of Congress (which appears increasingly derelict in the duty to address cyber threats to national security) but has been made almost incomprehensibly by default. As a result, the nation lacks a plan to address cyber threats of a severity that could disrupt the BPS into widespread, long-duration outages. In the absence of a plan—or concerted federal legislation to address the risks—

30. Regarding the long lead time required to procure heavy BPS equipment from off-shore manufacturers, note the following:

> Estimates are that most first world economies can cope for 3–4 days without power. Anything more than that, and social order dies a rather quick death. Given that most of the huge and complex power generators are built in China and India and have rather a long lead-time to produce (anywhere from months to years), a powerless Australia for up to a year [from a destructive cyber attack] is a daunting prospect.

Katherine Ziesing, *The Cyber Bogeyman*, STRATEGIST (June 18, 2013), http://www.aspistrategist.org.au/the-cyber-bogeyman/.

31. STEWART BAKER ET AL, CTR. FOR STRATEGIC & INT'L STUDIES, IN THE DARK: CRUCIAL INDUSTRIES CONFRONT CYBERATTACKS 2 (2011), *available at* http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf.

private industry has had no choice but to add this risk to the other risks that critical infrastructure boards oversee in order to ensure that senior management recognize, assess, and responsibly address cyber risks.

The boards of directors of companies that operate critical infrastructure have struggled over the past few years to understand these new responsibilities and to determine how to fulfill their fiduciary duties to oversee management's efforts to identify, assess, and address the cyber risks.[32] But a major impediment they

32. Direct evidence of these difficulties would be confidential and proprietary to each board; however, indirect evidence can be reasonably inferred from the fact that critical infrastructure company boards are well aware that their fiduciary duties include addressing any serious risks and threats to the enterprise, including those that originate with kinetic cyber attacks. Delaware corporate law, for example, requires boards to keep informed of serious risks to the enterprise. *See* Steven L. Caponi, *Cybersecurity and the Board of Directors: Avoiding Personal Liability—Part II of III*, KNOWLEDGE EFFECT (Aug. 6, 2013), http://blog.thomsonreuters.com/index.php/cybersecurity-and-the-board-of-directors-avoiding-personal-liability-part-ii-of-iii/ ("The failure to exercise appropriate oversight in the face of known risks constitutes a breach of the duty of loyalty, a breach that cannot be exculpated under 8 Del. C. § 102(b)(7).").

However, the evidence of the lack of significant improvement in cybersecurity among critical infrastructure companies suggests, not that boards are ignoring the issue, but that they and management have been struggling to address the cybersecurity risks in balance with other risks that warrant their attention. Thus, a recent survey by FTI Consulting found strikingly contradictory results when comparing knowledge of cybersecurity risks, particularly to operations, with significant success in addressing the risks. For knowledge of the risks the survey found: 55% of general counsel said that data security was their top concern," and "47% of general counsel said that operational risks, such as cybersecurity, were their most pressing concern." *Id.*

But for success in addressing the risks the survey found: "33% of general counsel believe that boards are not adequately managing cyber risk." *Id.* These findings are not an isolated or a one-off result. A report by a major law firm a *year* later, in 2012, similarly observed:

> [A] recent survey of 1,957 general counsel and 11,340 corporate directors indicated that cybersecurity and data protection for the first time rank as top-of-mind concerns, edging out perennial priorities like operational risk and [Federal Corrupt Practices Act] compliance. But now that the issues are on boards' radar screens, to what should limited corporate resources be directed so that key business assets are protected and legal and other risks are minimized? Unsurprisingly given the emerging nature of the challenge, the answer to how business should address cybersecurity-related risk is evolving.

HOGAN LOVELLS, CYBERSECURITY: THE CORPORATE COUNSEL'S AGENDA 3 (2012)

continuously encounter is who has the responsibility for cybersecurity. Moreover, to the extent that standards for that responsibility are emerging, they are coming from different sources, with discrepant objectives, and they implicate different responsibilities for a board and senior management.[33] As a result, if

(footnote omitted), *available at* http://www.hoganlovells.com/custom/eDocs/Cybersecurity%20Advisory_Pearson_11152012.pdf. The report continued, "A strong consensus thus has emerged in the United States that neither the private sector nor government is doing enough." *Id.* at 7.

Perhaps most telling are sector-specific findings concerning preparations to address kinetic cyber attacks against critical infrastructure company operations. Another study's conclusion further attests to the struggle that boards and management would appear to be having in addressing the risks and threats from coordinated cyber attacks designed to have kinetic effects:

> [I]ndustry executives made modest progress over the past year [2010–11] in securing their networks—adopting about half of the security technologies we identified. The energy sector increased its adoption of security technologies *by a single percentage point, to 51 percent,* while oil and gas executives reported an increase of 3 percentage points, to 48 percent. . . .
>
> Almost exactly the same pattern held true when we asked about adoption of security measures for respondents' Industrial Control (ICS) or Supervisory Control and Data Acquisitions (SCADA) systems. . . . They are doing something—but only a little more than they were doing last year.

BAKER ET AL., *supra* note 31, at 1 (emphasis added).

Further, "[b]etween one fifth and a third of all respondents told us that their company was not at all prepared, or not very prepared, for cyberattacks ranging from malware to denial-of-service—a figure that has not improved much since last year." *Id.*

33. One reason for the lack of clear guidance may be that one of the nation's most prominent regulators of critical infrastructure companies in the energy sector has questioned publicly whether the agency has the authority to issue and enforce cybersecurity regulations and standards. Federal Energy Regulatory Commission (FERC) former Chairman Jon Wellinghoff stated that the Commission has no such authority, that authority can only come from Congress, and that Congress has not enacted a statute to provide it. As then-Chairman Wellinghoff explained in a September 2012 speech:

> No. 1, I don't have an effective way to confidentially communicate [cyber threats] to the utilities . . . . And No. 2, I have no effective enforcement authority, and I've said this for six years now. And I've also said I don't care who has the authority, but Congress should give someone the authority.

Zack Colman, *Official: Congress Must Establish Electric Grid Cybersecurity Authority*, THE HILL (Sept. 5, 2012, 3:25 PM), http://thehill.com/blogs/e2-wire/e2-wire/247635

a threat is reported against companies that operate the nation's critical infrastructure, the operators and owners of those companies will not only ask if the threat is credible, but if responsibility for addressing the threat rests with their company and its limited resources or with governmental authorities and their potentially vast resources, including access to threat intelligence and offensive cyber weapons.[34]

Adversaries can and have successfully attacked U.S. critical infrastructure.[35] However, the question of who is responsible for

-obama-official-congress-must-give-someone-electric-grid-cybersecurity-authority (quoting then-FERC Chairman Jon Wellinghoff). But Congress, while not yet enacting cybersecurity legislation per se, still gave FERC authority to establish an Electric Reliability Organization that establishes reliability standards. Specifically, the Electricity Modernization Act of 2005 (Energy Policy Act of 2005, Pub. L. No. 109-58, § 1211, 119 Stat. 594 (codified as amended at 16 U.S.C. § 8240 (2012))) added section 215 to the Federal Power Act (FPA), which authorized FERC to certify an organization as the national "Electric Reliability Organization," which would be charged with establishing and enforcing mandatory reliability standards. Alcoa Inc. v. Fed. Energy Regulatory Comm'n, 564 F.3d 1342, 1344 (D.C. Cir. 2009) (citing 16 U.S.C. § 824o(a)(2) (2006)). On January 18, 2008, FERC issued a Final Rule (Order No. 706) approving, pursuant to section 215 of the FPA, eight Critical Infrastructure Protection (CIP) Reliability Standards submitted to FERC for approval by the NERC. Mandatory Reliability Standards for Critical Infrastructure Protection, 73 Fed. Reg. 7368 (Feb. 7, 2008) (codified at 18 C.F.R. pt. 40). All eight of these CIP Standards cover cybersecurity mandates.

34. For owners and operators of critical infrastructure companies, the potential availability of federal coverage cannot be a reassuring prospect when Congress plays "shut down" for political leverage as if adversaries would never take advantage of the resulting vulnerabilities.

35. As noted in a 2013 Council on Foreign Relations Report:

> Cyber threats to oil and gas suppliers pose an increasingly challenging problem for U.S. national security and economic competitiveness. Attacks can take many forms, ranging from cyber espionage by foreign intelligence services to attempts to interrupt a company's physical operations. These threats have grown more sophisticated over time, making them more difficult to detect and defend against. So, too, have the actors behind them, which have evolved from lone hackers with few resources to state-sponsored teams of programming experts. Several of the world's major oil and gas producers, including Saudi Aramco (officially the Saudi Arabian Oil Company) and Qatar's RasGas, have fallen victim to cyberattacks since 2009. Others, such as Chevron, have also had their networks infected.
>
> Some damage was done in each of these cases, but the costs of future breaches could be much higher, whether to corporate assets,

addressing the attack and averting future similar attacks remains stubbornly unclear. Often, the Department of Defense (DoD) has played little or no role (or no publicly disclosed role) in defending critical infrastructure companies from these attacks.[36] The responsibility for defending a critical infrastructure company from offshore kinetic cyber attacks, for determining whether a reported threat is credible, and for determining what preparations should be made in light of the reported threat arguably rests more with its board of directors than the Joint Chiefs of Staff, and more with its C-level officers than U.S. Central Command officers.

The executive branch and the BPS regulator, NERC, have attempted through recent initiatives to remove some of the uncertainties that confront BPS company boards and management in their efforts to address cyber attack risks to their enterprises.

The White House cybersecurity initiatives came out on February 12, 2013, when the president issued the EO entitled *Improving Critical Infrastructure Cybersecurity*[37] and the related Presidential Policy Directive 21 (PPD-21).[38] Since then, critical infrastructure boards have asked counsel to help them understand what, if anything, their industries are doing and what their companies' legal obligations are in response to the EO and its

> public infrastructure and safety, or the broader economy through energy prices.

BLAKE CLAYTON & ADAM SEGAL, COUNCIL ON FOREIGN RELATIONS, ENERGY BRIEF: ADDRESSING CYBER THREATS TO OIL AND GAS SUPPLIERS 1 (2013), *available at* http://i.cfr.org/content/publications/attachments/Energy_Brief_Clayton_Segal.pdf.

36. For example, one of the most successful cyber-attack campaigns against U.S. critical infrastructure companies targeted oil and gas firms (an attack dubbed "Night Dragon" by McAfee, the company that discovered and disclosed it). According to McAfee:

> Night Dragon was a "coordinated, covert, and targeted" campaign by China-based hackers to obtain confidential data from five major Western energy companies, beginning around 2008 and extending into early 2011. Night Dragon was able to steal gigabytes of highly sensitive material, including proprietary information about oil- and gas-field operations, financial transactions, and bidding data.

Id. at 1–2.

37. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

38. Presidential Policy Directive/PPD-21: Directive on Critical Infrastructure Security and Resilience, 2013 DAILY COMP. PRES. DOC. 92 (Feb. 12, 2013) [hereinafter PPD-21], *available at* http://www.gpo.gov/fdsys/pkg/DCPD-201300092/pdf/DCPD-201300092.pdf.

implementation of a two-pronged strategy: development of the Cybersecurity Framework (i.e., a collection of industry standards and best practices to be drafted by the National Institute of Standards and Technology (NIST) and recommended to critical infrastructure owners and operators for their "voluntary" adoption) and issuance of federal cyber intelligence reports to be shared with critical infrastructure companies.

However, such questions may need to be revised to address a significant and widening discrepancy between cybersecurity objectives pursued by the White House and cybersecurity objectives pursued by NERC. The White House's cybersecurity objectives appear, from the EO and PPD-21, to be the improvement of cyber defenses and critical infrastructure resilience against cyber attacks.

By contrast, NERC's cybersecurity objectives (beyond those expressed in the Critical Infrastructure Protection (CIP) Standards) appear to focus on managing the BPS operating crisis that would follow a disruptive and damaging kinetic cyber attack on BPS companies. NERC Task Forces discuss such an incident by referring to it as a Severe Event—one in which the damage was so extensive and so far beyond any previously experienced by operators and owners of BPS companies that full restoration of electric power could not be achieved for months or years.

As NERC Task Forces have described it, an attack may cause such extensive disruption and damage to BPS operations that it probably would result in operating isolated "islands" of electricity, scheduling rolling outages to maintain those "islands" while trying to bring new "islands" back on line with "black start"[39] resources

39. "Black start" is defined as

> the ability of a generating unit to start without an outside electrical supply, or is the demonstrated ability of a generating unit with a high operating factor to automatically remain operating at reduced levels when disconnected from the grid. Black start service is necessary to help ensure the reliable restoration of the grid following a blackout.

Glossary, ELEC. STORAGE ASS'N, http://energystorage.org/energy-storage/glossary/b (click "Black start") (last visited Dec. 27, 2013). FERC uses the term "black start service" with a somewhat different emphasis. FERC describes such "service" as allowing "a generating unit to start without an outside electrical supply or to continue operating at reduced levels when disconnected from the grid, and is needed for restoration of the transmission system in the event of a de-energizing event (e.g., a blackout)." PJM Interconnection, L.L.C., 144 FERC ¶ 61,191, at 1 n.2 (2013).

able to start generation without power supply to operate control systems and fuel ignition systems—in short, a grid fractured into an archipelago of illuminated islands surrounded by vast areas, populations, and regional economies without power or with power only in rotating shifts: four hours on, four hours off. We doubt that most BPS companies have had time or made it a priority to prepare for such far-reaching and unfamiliar consequences. If BPS companies have failed to prepare, it is reasonable to infer that most, if not all, critical infrastructure companies have yet to make such preparations or even to grasp the post-attack consequences that NERC's Task Forces have identified after careful review of the probable operational impacts.

Unlike the White House's initiatives, which seem to offer the possibility of a successful defense, NERC's cybersecurity initiatives assume that such defenses will ultimately be breached and that the highest priority should be to prepare to manage the consequences of a period of "New Normal" during which the grid would have to be operated at reduced levels of electric power with power being available only in multiple separate "islands" and requiring rolling outages in order to stabilize electric service within such "islands." This is the objective set forth by the NERC Task Force reports that the NERC Board of Trustees approved on May 9, 2012—nine months before the President issued the EO.[40]

Thus, the White House and NERC have surprisingly different objectives for their respective cybersecurity initiatives, and the gap between them appears to be widening because little, if any, attention is being given by the White House or NERC to coordinating those different objectives. Moreover, the White House and NERC do not appear to recognize that the BPS boards and management may find it financially and organizationally impracticable to pursue both sets of objectives. As a result, the BPS boards and management will need to choose which set of objectives to devote their resources and efforts to achieving—the objectives identified by the White House in the EO and Cybersecurity Framework or the objectives identified by the NERC Task Force reports. As boards recognize the divergence between those objectives, they may find the decision between such objectives difficult to make because pursuing either at the expense of the

40. *See* CATF REPORT, *supra* note 13; SIRTF REPORT, *supra* note 13.

other could increase the exposure of the company, its management, and its board to post-cyber attack liability for failure to address cybersecurity risks responsibly.

We believe that BPS company boards and management need to grasp the new operating environment that would result from a successful kinetic cyber attack against the BPS, and that those consequences pose the greatest risks to a BPS company and its operations, as well as to its finances, reputation, and survival.

Responding responsibly to the White House initiatives will *not* suffice as a response to the NERC Task Forces' initiatives. Many companies may find that they cannot allocate equal resources and oversight to make the preparations called for by the White House and those called for by their regulators. That recognition will create considerable tension for a board as it may force the board and management to choose whether to place the company's priorities on responding to the White House or to the relevant sector regulator. Of course, in some sectors, including energy, such a choice would potentially expose the company to penalties that can accrue at the rate of one million dollars per day per violation, so complying with NERC requirements is mandatory whereas White House recommendations may be more aspirational.[41]

41. In the Energy Policy Act of 2005, "Congress added section 215 to the Federal Power Act (FPA) [16 U.S.C. § 824o (2012)], which provides for the creation of a national Electric Reliability Organization [which is NERC] charged with establishing and enforcing" mandatory reliability standards. Alcoa Inc. v. Fed. Energy Regulatory Comm'n, 564 F.3d 1342, 1344 (D.C. Cir. 2009). Section 215 authorizes the Electric Reliability Organization (ERO) to impose penalties for violations of reliability standards against "a user or owner or operator of the bulk-power system," subject to FERC review. 16 U.S.C. § 824o(e)(1). Title 16 U.S.C. § 824o(b)(1) extends FERC's jurisdiction for "enforcing compliance" with reliability standards to "all users, owners and operators of the bulk-power system." In February of 2006, "FERC issued Order No. 672 to implement section 215." *Alcoa Inc.*, 564 F.3d at 1344; *see* Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing, 116 FERC ¶ 61,062 (July 20, 2006), *reh'g denied*, Order on Petitions for Rehearing and Clarification; Order on Compliance Filing, 117 FERC ¶ 61,126 (Oct. 30, 2006), *review denied*, *Alcoa Inc.*, 564 F.3d at 1342. FERC certified NERC as the national Electric Reliability Organization. Section 316A of the FPA imposes a statutory cap on monetary penalties of one million dollars per day, per violation, for violations of electric reliability standards. 16 U.S.C. § 825o(1). Unlike section 316A, section 215 does not specify a monetary cap on FERC's or NERC's penalty authority. Therefore, in Order No. 672—in the absence of a monetary cap in

We think that the NERC objectives and accompanying recommendations seem better suited for protecting critical infrastructure from the worst-case scenarios.[42] We therefore argue in this essay that, from a national security perspective, critical infrastructure is best protected by preparing for cyber defenses to fail and for incident response and recovery to be impaired and by concentrating efforts on managing the resulting crisis of months of reduced operation and service by critical infrastructure.[43]

In the next two sections, we explore the kinds of reports or notices of cyber attack threats that NERC Task Force initiatives (beginning in May 2012) and the White House initiatives (beginning in February 2013) are bringing to the attention of boards and management of critical infrastructure companies. In each section, we analyze the challenges that such reports or notices create for boards and management as they seek to determine the scope of their responsibilities for addressing those threats and risks.

IV. THE EVOLVING CYBERSECURITY REGULATORY CONTEXT

In this section we discuss the emerging cyber threats to critical infrastructure, the identification and assessment of the most serious threats to the BPS, and the curiously different threats that the White House and NERC have focused on in their respective cybersecurity initiatives for critical infrastructure.

A. Remotely Launched, Kinetic Cyber Attacks Against Critical Infrastructure Become Possible

Prior to 2007, cyber threats to most companies involved attacks to exfiltrate valuable information (business plans, financial data, source code, patentable inventions, trade secrets and other intellectual property, etc.)—a trend that continues through the

section 215—FERC determined that section 215 penalties should be subject to the same monetary caps that apply to civil penalties under section 316A. Order Denying Rehearing, 141 FERC ¶ 61,242, ¶ 50 (Dec. 20, 2012) (citing Order No. 672: Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards, 71 Fed. Reg. 8662 (Feb. 17, 2006) (codified at 18 C.F.R. pt. 39)). Section 316A of the FPA applies to any FPA-related violation, whether the monetary penalty is levied by FERC, NERC, or a regional entity.

42. *See supra* text accompanying notes 38–39; *infra* Part IV.F–G.

43. *See infra* Part V.

present.[44] The motives usually appeared to be financial gain, commercial advantage, and industrial and economic espionage.[45] The targets were usually a company's business information systems, since that is where the targeted data tended to be stored.

At least as early as the spring of 2007, the perception of the nature of cyber threats to operations of critical infrastructure underwent a "sea-change." Evidence of this change in threat perception appeared in NERC's first distribution of a "cyber-vulnerability alert" prepared by the Department of Homeland Security (DHS) to certain BPS companies. The alert (dubbed "Aurora")

> was intended to caution the industry to secure remotely accessible transmission relays and other devices from cyber attack. The perceived threat was based on simulations conducted at Idaho National Laboratory in December 2006, which demonstrated the possibility of

44.

> Cyber attacks generally refer to criminal activity conducted via the Internet. These attacks can include stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet and disrupting a country's critical national infrastructure. Consistent with the previous two studies, the loss or misuse of information is the most significant consequence of a cyber attack. Based on these findings, organizations need to be more vigilant in protecting their most sensitive and confidential information.

PONEMON INST., 2012 COST OF CYBER CRIME STUDY: UNITED STATES 1 (2012), *available at* http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

45. For example, in December 2007, Britain's MI5 issued an alert "to 300 chief executives and security chiefs at banks, accountants and legal firms" warning that "Chinese state organizations" were targeting them for cyber attacks aimed at espionage with a goal of "steal[ing] confidential commercial information." *Britain's MI5: Chinese Cyberattacks Target Top Companies*, FOX NEWS (Dec. 3, 2007), http://www.foxnews.com/story/2007/12/03/britain-mi5-chinese-cyberattacks-target-top-companies/.

Also, as noted in a study that considered attacks against military and non-military entities, cyber espionage creates commercial advantage for competitors who gain information from the intruders: "We cannot accurately assess the dollar value of the loss in military technology but we can say that cyber espionage . . . shifts the terms of engagement in favor of foreign competitors." JAMES LEWIS ET AL., CTR. FOR STRATEGIC & INT'L STUDIES, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE 4 (2013), *available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

> remotely accessing bulk power system (BPS) relays to damage rotating machines—such as generators, pumps or motors—that are connected to the power grid.[46]

As cybersecurity expert Bruce Schneier explained at the time, the attack demonstration was launched remotely and destroyed a vital part of the rotating machinery:

> [T]hey were unable to hurt the generator you see in the video but did destroy the shaft that drives it and the power unit. They triggered the event from 30 miles away! Then they extrapolated the theory that a malfunctioning generator can destroy not only generators at the power company but the power glitches on the grid would destroy motors many miles away on the electric grid that pump water or gasoline (through pipelines).[47]

Despite issuing the Aurora alert in Spring 2007, neither NERC nor its BPS member operators and owners made substantial changes in their cybersecurity practices, as if the alert were no more credible (and no less accurate) than a warning from a contemporary Cassandra.[48] As a Congressional report critically observed in May 2013, NERC initiatives on cybersecurity do not appear geared to keep pace with the accelerating rapidity of the emerging cyber threats.[49]

46. *Bulk Power System Cyber Security*, AM. PUB. POWER ASS'N 1 (Feb. 2013), http://www.publicpower.org/files/PDFs/BulkPowerCyberSecurityFeb2013IB.pdf.

47. Bruce Schneier, *Staged Attack Causes Generator to Self-Destruct*, SCHNEIER ON SECURITY (Oct. 2, 2007, 6:26 AM), https://www.schneier.com/blog/archives/2007/10/staged_attack_c.html (citing an anonymous email received regarding the Idaho National Laboratory video).

Note that later, in the same blog post, Schneier asserts that "the vulnerability they hypothesize is completely bogus but I won't say more about the details. Gitmo is still too hot for me this time of year." *Id.* However, he may have reconsidered that view once reports of the success of Stuxnet emerged in 2010.

48. In Greek mythology, Cassandra was a daughter of Priam, King of Troy depicted in the Iliad. The god Apollo endowed her with the gift of prophecy, but also deemed that no one would ever believe her prophecies. She prophesied the fall of Troy, and the Trojans refused to believe her. In contemporary English, a "Cassandra" is thus "anyone who expresses pessimistic views of the political or social future and is not listened to." THE CHAMBERS DICTIONARY 263 (1993).

49. The report noted that

> NERC's record with regard to taking prompt action on grid security vulnerabilities and threats has raised concerns. For example, more than six years after the identification of the Aurora vulnerability discussed above, NERC still has not proposed any reliability standard

B. Stuxnet Worm Demonstrates Effectiveness of Remotely Launched, Kinetic Cyber Attacks Against Critical Infrastructure

Simulations in a domestic national lab—and warnings issued on that basis—are one thing. It's quite another thing when a cyber attack is tried against a major facility and works, damaging critical equipment and disrupting operations and product output.[50] When that happened with the extraordinarily sophisticated, complex, stealthy, and potent worm launched against a major Iranian uranium processing facility with destructive consequences, the "handwriting was on the wall"—the cyber world had transitioned from science fiction and theoretical imaginings of an ominous

> directly addressing that vulnerability. Moreover, NERC's CIP standards only apply to assets identified by utilities as critical.

STAFF OF CONGRESSMEN EDWARD J. MARKEY & HENRY A. WAXMAN, 113TH CONG., ELECTRIC GRID VULNERABILITY: INDUSTRY RESPONSES REVEAL SECURITY GAPS 8 (May 21, 2013), *available at* http://democrats.energycommerce.house.gov/sites/default/files/documents/Report-Electric-Grid-Vulnerability-2013-5-21.pdf.

The arguably limited benefit of the CIP Standards to protect the BPS is evidenced also by the fact that "[p]ower plants under 1,500 MW are excluded even though that eliminates 70%–80% of the generation in North America." David Savenije, *Could a Cyberattack Take Out the U.S. Power Grid Today?*, UTILITY DIVE (Sept. 6, 2013), http://www.utilitydive.com/news/could-a-cyberattack-take-out-the-us-power-grid-today. "The entire distribution network is excluded, as well as small transmission assets." *Id.*

50. Since 2007, as the ability to carry out kinetic cyber attacks has grown, so have efforts to use cyber tools to remotely collect intelligence about government organizations, military and defense sites, and energy sector company operations. As noted in a timeline posted on the website of *NATO Review Magazine*, such attacks have recently been widespread, and although they date back to 2007, their continuing exploits have only recently been discovered and disclosed publicly:

> The Russian firm Kaspersky discovered a worldwide cyber-attack dubbed "Red October," that had been operating since at least 2007.
>
> Hackers gathered information through vulnerabilities in Microsoft's Word and Excel programmes [sic]. The primary targets of the attack appear to be countries in Eastern Europe, the former USSR and Central Asia, although Western Europe and North America reported victims as well.
>
> The virus collected information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures.

The History of Cyber Attacks—A Timeline, NATO REV. MAG., http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm (select the "October 2012" entry on the timeline to access the quoted language) (last visited Dec. 27, 2013) (emphasis omitted).

future into a vivid demonstration of credible long-range, weapons-grade cyber threats.[51] The delivery system and its malware payload were dubbed "Stuxnet."[52]

Stuxnet's effective attacks caused the Iranian uranium enrichment centrifuges at the Natanz facility to accelerate and decelerate at preset fifteen-minute intervals so that they rotated or spun at speeds above and below their specified operating range and then back within it (to disguise the disruption from the operators) until the centrifuges degraded and self-destructed. As explained in a *Scientific American* essay:

> Under normal operating conditions, the centrifuges spin so fast that their outer edges travel just below the speed of sound. Stuxnet bumped this speed up to nearly 1,000 miles per hour, past the point where the rotor would likely fly apart, according to a December report by the Institute for Science and International Security. At the same time, Stuxnet sent false signals to control systems indicating that everything was normal.[53]

The damage disrupted the facility's product output for an extended period.[54] Stuxnet reportedly caused over 900 rotating centrifuges at Natanz to self-destruct and severely damaged the rotating steam turbine in the Bushehr nuclear power plant.[55] Initial reports of the discovery of Stuxnet appeared in June 2010.[56]

51. *See* NICHOLAS FALLIERE ET AL., SYMANTEC SEC. RESPONSE, W32.STUXNET DOSSIER 1 (version 1.3, 2010), *available at* http://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf.

52. *Id.*

53. David M. Nicol, *Hacking the Lights Out*, SCI. AM., July 1, 2011, at 70, 71 (arguing that the BPS "shares many of the vulnerabilities that Stuxnet exposed; being larger, its vulnerabilities are, if anything, more numerous").

54. *See What Stuxnet Is All About*, LANGNER (Jan. 10, 2011), http://www.langner.com/en/2011/01/10/what-stuxnet-is-all-about/.

55. *See* Ed Barnes, *Stuxnet Worm Still Out of Control at Iran's Nuclear Sites, Experts Say*, FOX NEWS (Dec. 9, 2010), http://www.foxnews.com/scitech/2010/12/09/despite-iranian-claims-stuxnet-worm-causing-nuclear-havoc/ ("The Stuxnet worm . . . was equipped with a warhead that targeted and took over the controls of the centrifuge systems at Iran's uranium processing center in Natanz, and it had a second warhead that targeted the massive turbine at the nuclear reactor in Bashehr.").

56. FALLIERE ET AL., *supra* note 51, at 4; PAUL K. KERR, JOHN ROLLINS & CATHERINE A. THEOHARY, CONG. RESEARCH SERV., THE STUXNET COMPUTER WORM:

However, it appears that Stuxnet was launched two years earlier and had been infecting the Natanz enrichment plant and the Bushehr nuclear power plant for a year without the Iranian government's (or the facilities' operators') awareness of the malware's presence and stealthy conduct of sabotage in the facilities' computer networks and system control and data acquisition (SCADA) systems.[57]

Stuxnet's makers apparently discovered that these plants were vulnerable to a cyber attack, not because the operational machinery and enrichment centrifuges are connected to the Internet—which they apparently are not—but because both plants' operations and processes are monitored and controlled by SCADA systems, designed and manufactured by Siemens.[58] The SCADA system, in turn, is operated by a "specialized assembly like code on programmable logic controllers (PLCs)."[59] These PLCs tend to be programmed from Windows computers that also are not connected to the Internet (and certainly do not need to be Internet-connected).[60] The Stuxnet makers appear to have designed the malware to exploit vulnerabilities in the PLCs to then exploit vulnerabilities in the SCADA systems—tasks that required considerable intelligence on the PLCs and SCADA systems in these plants.[61]

Equally alarming for operators and owners of critical infrastructure that depend on heavy equipment with spinning or rotating parts, Stuxnet not only hid its presence, but also created what is known as a "man-in-the-middle" attack to conceal from the SCADA system and plant operating personnel the unauthorized changes it was causing to the operations of the centrifuge motors.[62] Stuxnet took over the devices controlling the input to and output

HARBINGER OF AN EMERGING WARFARE CAPABILITY 1 (2010), *available at* http://www.fas.org/sgp/crs/natsec/R41524.pdf.

57. *See The Short Path from Cyber Missiles to Dirty Digital Bombs*, LANGNER (Dec. 26, 2010), http://www.langner.com/en/2010/12/26/the-short-path-from-cyber-missiles-to-dirty-digital-bombs/.

58. *See* FALLIERE ET AL., *supra* note 51, at 3, 4.

59. *Id.* at 3.

60. *Id.*

61. *See id.*

62. Ralph Langner, *How to Hijack a Controller: Why Stuxnet Isn't Just About Siemens' PLCs*, CONTROL (Jan. 13, 2011), http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html.

from the centrifuges, without the controller devices recognizing it.[63] Stuxnet did the same to the data being reported by the system to the operators: it substituted data it created, making it appear to the controller that the centrifuges were operating within their specified upper and lower ranges when in fact they were spinning at first too rapidly and then too slowly, destroying themselves in the process. As one analyst explained: "It's just like you have seen it in movies where the bad guys feed observation cameras with unsuspicious pre-recorded video."[64]

C. Vulnerabilities of BPS Facilities to Remotely Launched, Kinetic Cyber Attacks

By disguising the data input and output from the controlling devices and the plant operators, Stuxnet could carry out the ultimate aggressive cyber attack.[65] Critical infrastructure plans often require continuous adjustment to operate properly—that is particularly true of BPS facilities.[66] As explained in an MIT study, entitled *The Future of the Electric Grid*:

> The electric power system is operated through a combination of automated control and actions that require direct human (system operator) intervention. The main challenge in operating the electric power system is that there is negligible "electrical" storage in the system. Hence, supply and consumption of electrical power must be balanced at all times. Since the load is changing all the time in ways that cannot be perfectly predicted, generation must follow the load in real time. The balance between supply and demand is maintained using a hierarchical control scheme, with crude matching at the

63. *See* FALLIERE ET AL., *supra* note 51, at 12–14.

64. *417 Attack Code: Doing the Man-in-the-Middle ON the PLC*, LANGNER (Nov. 15, 2010), http://www.langner.com/en/2010/11/15/417-attack-code-doing-the-man-in-the-middle-on-the-plc/.

65. For further discussion of Stuxnet and its relation to cybersecurity for nuclear power plants, see Roland L. Trope & Geoffrey Schwartz, Cyber Security for U.S.-Based Nuclear Power Plants (Jan. 2011) (unpublished manuscript) (on file with author) (essay for continuing legal education program, ABA Cyberspace Law Committee's annual Cyberspace Law Institute).

66. MASS. INST. OF TECH., *supra* note 1, at 253–54.

> longer timescale and finer matching at the shortest timescale . . . .[67]

Unlike operations in many other industries, the "balancing" activities required to maintain stable operations in a BPS company require not only "24x7" monitoring, but close attention to the rapid, moment-to-moment changes in the electricity demand and supply that need to be continuously balanced—whenever they tip out of balance, they must be restored within seconds to avert tripping off cascading outages. In short, the operations must constantly protect the system from throwing itself out of balance and causing the company to fail to maintain the reliability of electric power required by the regulators to keep the system from degrading into blackouts. As the MIT study further explains:

> An important aspect of the operation of the electric power system is protection. This means ensuring the safety of the system, including generating units and other grid assets, and the people who may come in contact with the system. Protective action must be taken in fractions of a second to avoid equipment damage and human injury. Protection is achieved using sensing equipment as well as circuit breakers and other types of switches that can disconnect and de-energize parts of the system in the case of a fault, such as a damaged transmission line or a short circuit. . . .
>
> . . . Computers are regularly calculating system power flows and voltages under various possible contingencies, for example[,] the failure of a large generator or transmission line, to identify the best corrective action to take in each case.
>
> . . . [R]eal-time operation of the electric power system . . . ensure[s] that the system remains stable and protected while meeting end user power requirements. This requires a precise balance between power generation and consumption at all times. If this balance is not maintained the system can become unstable—its voltage and frequency can exceed allowable bounds—and result in damaged equipment as well as blackouts. If the balance is not restored sufficiently quickly, a local blackout can

67. *Id.* at 254 (footnote omitted).

grow into a cascading blackout similar to the ones in the U.S. in 1965 and 2003.[68]

The operators must therefore maintain and continuously update their situation awareness of a BPS facility's equipment and electrical load balances so that if something starts to malfunction or electrical power generation and consumption begins to go out of balance the operators can start to correct it within a few seconds.[69] Any delay or error in the response could trigger cascading problems within the facility and to other parts of the interconnected BPS. The start of cascading outages that led to the August 2003 blackout across the Northeast United States and a Canadian province apparently could have been halted by operator intervention before it became widespread, but a "failure of the alarm processor in the control system of FirstEnergy, an Ohio-based electric utility, prevented control room operators from having adequate situational awareness of critical operational changes to the electrical grid."[70]

68. *Id.* at 254–55.

69. The general public and even most owners and operators of critical infrastructure tend to be unaware of or underestimate the precise, moment-to-moment balancing required to maintain the reliability of a transmission grid like the BPS. NERC and its ten Regional Reliability Councils base their system operating and planning standards for ensuring grid reliability on seven crucial concepts:

- Balance power generation and demand continuously.
- Balance reactive power supply and demand to maintain scheduled voltages.
- Monitor flows over transmission lines and other facilities to ensure that thermal (heating) limits are not exceeded.
- Keep the system in a stable condition.
- Operate the system so that it remains in a reliable condition even if a contingency occurs, such as the loss of a key generator or transmission facility . . . .
- Prepare for emergencies.

U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, *supra* note 6, at 6–7.

70. *Cybersecurity Challenges in Securing the Modernized Electricity Grid: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 112th Cong. 10–11 (2012) (statement of Gregory C. Wilshusen, Director of Information Security Issues), *available at* http://www.gao.gov/assets/590/588913.pdf. Note, however, a different view is provided by the definitive study of the causes of the August 2003 blackout, which concluded that four causes combined to trigger it, including "[i]nadequate situational awareness at

An adversary planning a coordinated cyber attack against a BPS installation might attempt to disrupt, disorient, and mislead such real-time responses. If operators receive false information about equipment or system status (or information maliciously delayed to deprive it of its real-time accuracy and insight as needed for situational awareness[71]), they may fail to react in time (as happened during the Stuxnet attack) or they could be fed data to cause them to take the wrong—and thus damaging—corrective action (e.g., shedding electric loads when digital readouts indicate erroneously—at the direction of malware—that demand is slumping when it is, in fact, surging).[72]

FirstEnergy. FE did not recognize or understand the deteriorating condition of its system." U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, *supra* note 6, at 18.

71. Nicol, *supra* note 53, at 74–75.

> Attackers could . . . simply attempt to delay messages traveling between control stations and substations. Ordinarily the lag time between a substation's measurement of electricity flow and the control station's use of the data to adjust flows is small—otherwise it would be like driving a car and seeing only where you were 10 seconds ago. (This kind of lack of situational awareness was a contributor to the Northeast Blackout of 2003.)

Id.

72. As explained in a recent research paper on cyber attacks against the smart grid:

> An important class of cyber attacks are *data integrity* attacks. These consist of a set of compromised sensors (ex: power meters, relays) whose readings are altered by the attacker. . . .
>
> Data integrity attacks are of consequence only when the system operator reacts to the compromised data and is misled into taking uneconomical or even catastrophic decisions.

Annarita Giani et al., *Metrics for Assessment of Smart Grid Data Integrity Attacks, IEEE Power & Energy Society General Meeting: Energy Horizons–Opportunities and Challenges*, IDAHO NAT'L LABORATORY 1 (2012), *available at* http://www.inl.gov/technicalpublications/Documents/5517252.pdf (pre-print).

> Intuitively the physical violation occurs when the data integrity attack increases load at bus 7 (decreasing load at bus 8). This causes the operator to think it can cheaply dispatch generation at bus 7 to satisfy the extra load at bus 7. As this extra load does not actually exist, the excess generation is shipped on the already saturated line (7, 8), causing an overload.

Id. at 6.

D. Recently Discovered Vulnerabilities of BPS SCADA Systems

These risks are not theoretical and certainly not limited to the world of espionage, as in the Stuxnet attack. Rather, as several engineers recently demonstrated repeatedly, vulnerabilities can be exploited and systems disabled in the communication protocol used by power and water utilities to remotely monitor substations and other infrastructure. In April 2013, engineers Adam Crain and Chris Sistrunk tested open-source software used in such utility SCADA systems and found that a widely used program called DNP_3 was vulnerable to cyber attack. The engineers demonstrated that a software product of Triangle MicroWorks, which uses DNP_3, was vulnerable to cyber attack, allowing an attacker to infiltrate a power station's control center from afar with the ability to take over the system and mask its entry, even bypassing traditional firewalls.[73] Despite the engineers' prompt report of the vulnerabilities to ICS-CERT,[74] it took ICS-CERT four months to issue an alert and public advisory of the threats to critical infrastructure operators.[75] In issuing the alert, ICS-CERT emphasized that it was encouraging asset owners to take additional defensive measures to protect against this and other cybersecurity risks by:

- Minimizing network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locating control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, using secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.[76]

73. Nicole Perlroth, *The Electrical Grid Is Called Vulnerable to Power Shutdown*, N.Y. TIMES (Oct. 18, 2013), 2013 WLNR 26200409.

74. ICS-CERT is the acronym for the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team. *See* ICS-CERT, http://ics-cert.us-cert.gov/ (last visited Feb. 13, 2014).

75. *See* Advisory, ICS-CERT, Triangle MicroWorks Improper Input Validation (rev. Sept. 17, 2013), https://ics-cert.us-cert.gov/advisories/ICSA-13-240-01.

76. *Id.*

E. Chief Risks of Cyber Attacks Against BPS Companies Involve Targeting of Operational Systems

Aware of these risks and the growing sophistication of potential cyber attacks, NERC perceived that the chief cyber risks to the BPS would be attacks that targeted *operational systems, not business information systems*. NERC therefore developed successive versions of cybersecurity standards (known as Critical Infrastructure Protection or CIP Standards[77]) and that, upon approval by FERC, became mandatory on BPS operators in the United States.[78] Moreover, NERC took steps to identify the most serious threats—including cyber threats—to the reliability and resilience of the BPS. In July 2009, NERC and the U.S. Department of Energy (DoE) partnered on an effort to identify and address what became known as "high-impact, low-frequency" risks to the BPS.[79] A year later, in June 2010, NERC and DoE released a report on those risks, which included cyber attacks:

> The risk of a coordinated cyber, physical, or blended attack against the North American bulk power system has become more acute over the past 15 years as digital communicating equipment has introduced cyber vulnerability to the system, and resource optimization trends have allowed some inherent physical redundancy within the system to be reduced. The specific concern with respect to these threats is the targeting of multiple key nodes on the system that, if damaged, destroyed, or interrupted in a coordinated fashion, could bring the system *outside the protection provided by traditional planning and operating criteria*. Such an attack would behave very differently than traditional risks to the system in that an intelligent attacker could mount an adaptive attack that

77. *See Critical Infrastructure Protection Committee (CIPC)*, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/comm/CIPC/Pages/default.aspx (last visited Dec. 27, 2013); *see also* N. AM. ELECTRIC RELIABILITY CORP., RELIABILITY STANDARDS FOR THE BULK ELECTRIC SYSTEMS OF NORTH AMERICA (n.d.) [hereinafter BPS RELIABILITY STANDARDS], *available at* http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf (standards CIP-001-2a to -009-4).

78. On January 18, 2008, FERC issued a Final Rule (Order No. 706) approving, pursuant to section 215 of the FPA, eight CIP Reliability Standards submitted to FERC for approval by NERC. 73 Fed. Reg. 7368 (Feb. 7, 2008) (codified at 18 C.F.R., pt. 40).

79. *See* HILF REPORT, *supra* note 13.

> would manipulate assets and potentially provide misleading information to system operators attempting to address the issue.[80]
>
> A highly-coordinated and structured cyber, physical, or blended attack on the bulk power system, however, could result in long-term (irreparable) damage to key system components in multiple simultaneous or near-simultaneous strikes. . . . An outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods.
>
> . . . .
>
> The adversarial strategic advantage enjoyed by those targeting the bulk power system has been increased by the fact that sensitive information about critical bulk power system components and tools to carry out attacks are available and easily accessible in the public domain.[81]

The High-Impact, Low-Frequency Report identifies eight examples of cyber threats, including two that clearly recognize that adversaries could deploy the Stuxnet-like capabilities against the BPS:

- Unauthorized access attacks—attacks where the adversary exercises a degree of control over the system and accesses and manipulates assets without authorization
- Unauthorized use of assets, resources, or information—attack in which assets, services, or data are manipulated by an authorized user in an unauthorized manner. This can result in system operators being given inaccurate information from a 'trusted' source, and thereby being misled into making decisions based on this data that result in impacts to the system[82]

80. *Id.* at 10 (emphasis added).
81. *Id.* at 26–27.
82. *Id.* at 29 (footnote omitted).

F. The Severe Event Cyber Attack Damage to BPS Operations That NERC Task Forces Anticipate Surpasses the Damage from Cyber Attacks Anticipated by Executive Order 13636

If we compare the cyber threats and consequences anticipated by NERC and DoE, they appear to be far more severe than those identified by the President in the EO and PPD-21 several years later. During the period 2010–2013, however, NERC pressed forward to gain a greater understanding of the challenges that owners and operators of the BPS would face in the event that adversaries successfully launched the kind of attack foreseen by the High-Impact, Low-Frequency Report and that caused long-term damage to the grid and an impairment of the supply of electricity throughout the BPS. The NERC board approved a Coordinated Action Plan[83] and formed task forces to study such events and the probable consequences in order to come up with recommended preparations for owners and operators of BPS companies. Two reports emerged from these task forces. Both reports were accepted by NERC's Board of Trustees on May 9, 2012[84]—nine months before the issuance of the EO and PPD-21.

Interestingly, the 2012 NERC Task Force reports reflect a considerable advancement in NERC's identification and understanding of the nature of anticipated coordinated cyber attacks. In our experience and review of sources,[85] there are few

83. *See* N. AM. ELECTRIC RELIABILITY CORP., IMPLEMENTING THE COORDINATED ACTION PLAN 4 (2011), *available at* http://www.nerc.com/comm/Other/Critical%20Infrastructure%20Strategic%20Coordinated%20Acti/Implementing_CAP_Feb_2011.pdf.

84. CATF REPORT, *supra* note 13; SIRTF REPORT, *supra* note 13.

85. Among its distinguishing features, the Cyber Attack Task Force included wholesale power generation and electric transmission and distribution, infrastructure manufacturing, and grid operating expertise in the United States and Canada (both IT and operational), discussions with federal agencies and law enforcement, and incorporated lessons learned from current and past initiatives. CATF REPORT, *supra* note 13, at 1, 42–43. The Severe Impact Resilience Task Force consisted of a team of energy industry subject matter experts with capabilities to respond to emergency situations to reliably restore and operate the interconnected bulk power system and contributed expertise in areas including power system operation, transmission planning, generating plant operation, protection and control, distribution operations, communications, logistics, emergency planning, crisis response, and cyber and physical security. SIRTF REPORT, *supra* note 13, at 8, 125–30. The authors have found no other reports or

that offer such intelligent, thoughtful, and well-written descriptions of what the current capabilities of cyber attacks pose in the way of threats to the BPS.

The NERC Task Force report entitled *Cyber Attack Task Force* (the "CATF Report") cautions that without the experience of a successful coordinated cyber attack against the BPS, "it is difficult to confidently determine the potential impact on the reliability of the bulk power system and what additional actions may need to be taken"[86] by owners and operators to deal with the post-event damage, partial restoration of service, and prolonged recovery.[87] The CATF Report did not attempt to determine the likelihood of such an attack or to determine which functional entities might be more susceptible or vulnerable to attack. Instead, the CATF Report assumed that a coordinated cyber attack has occurred and adopted the following scenario to guide its work:

> An organized cyber disruption disables or impairs the integrity of multiple control systems, or intruders take operating control of portions of the bulk power system such that generation or transmission system[s] are damaged or operated improperly.
>
> 1. Transmission Operators report unexplained and persistent breaker operation that occurs across a wide geographic area (i.e., within state/province and neighboring state/province).
> 2. Communications are disrupted, disabling Transmission Operator voice and data with half their neighbors, their Reliability Coordinator, and Balancing Authority.
> 3. Loss of load and generation causes widespread bulk power system instability, and system collapse within state/province and neighboring state(s)/province(s). Portions of the bulk power system remain operational.
> 4. Blackouts in several regions disrupt electricity supply to several million people.[88]

analyses that have so comprehensively and collaboratively considered the potential impacts of a severe cyber attack on the bulk power system and the anticipated response, recovery, and restoration efforts that will be required.

86. CATF REPORT, *supra* note 13, at 1.

87. *Id.*

88. *Id.* at 2.

The success for an adversary in such a scenario (and indeed in any coordinated cyber attack against the BPS) depends on the occurrence of two events: "1) situational awareness needs to have been compromised and 2) there must be a bulk power system event or instability."[89]

The immediate and long-term consequences of such an attack were detailed in the NERC Task Force report entitled *Severe Impact Resilience: Considerations and Recommendations* ("SIRTF Report").[90] The SIRTF Report looked at three "high-impact, low-frequency" scenarios as the initiating events—one of which was a coordinated cyber attack—described as follows: "A coordinated disruption disables or impairs the integrity of multiple control systems, or intruders take operating control of portions of the BPS such that generation or transmission system is damaged or mis-operated."[91]

The SIRTF Report anticipated that such an attack would push BPS companies "beyond the emergency response capabilities entities typically have in place," resulting in a "Severe Event" and a post-attack "New Normal" for BPS operations.[92] The SIRTF Report defined a "Severe Event" as "an emergency situation so catastrophic that complete restoration of electric service is not possible." The BPS is operated at a reduced state of reliability and supply for months or possibly years through the New Normal period as illustrated below.

89. *Id.* at 12. The CATF Report explains that "Situational Awareness is impacted IF

- There is a Disruption / Compromise in Communications OR
- There is a failure of the Energy Management System or Generation Management System OR
- The Control Center is inaccessible or uninhabitable."

Id. at 13 (emphasis in original). The CATF Report also explains that "BPS Instability can occur IF

- There is a Loss/Change in Generation OR
- A Loss of Load OR
- A Disruption to Transmission or Distribution."

Id. (emphasis in original).

90. *See* SIRTF REPORT, *supra* note 13.

91. *Id.* at 1.

92. *Id.* at 2.

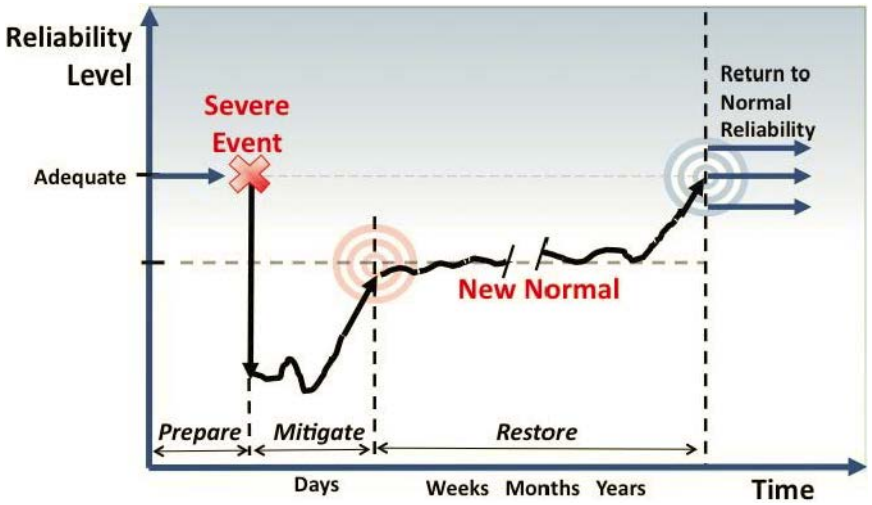

Figure 1[93]

A Severe Event would challenge BPS operators and owners because their companies would not be able to meet all electricity consumers' demands for rapid restoration of service.[94] Instead, they would have to prioritize customers and attempt to serve the highest

93. *Id.* at 2. This image from the North American Electric Reliability Corporation's website is the property of the North American Electric Reliability Corporation and is available at http://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF_FinalDraft_Feb_24_2012.pdf. This content may not be reproduced in whole or any part without the prior express written permission of the North American Electric Reliability Corporation.

Note that NERC's Task Force reports are not alone in foreseeing the duration of a post-attack, New Normal period of substantially reduced electric power. As one federal study reported in 2012:

> [I]f [a terrorist cyber attack] were carried out in a carefully planned way, by people who knew what they were doing, it could deny large regions of the country access to bulk system power for weeks or even months. An event of this magnitude and duration could lead to turmoil, widespread public fear, and an image of helplessness that would play directly into the hands of the terrorists. If such large extended outages were to occur during times of extreme weather, *they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold.*
>
> . . . .
>
> Electric systems are not designed to withstand or quickly recover from damage inflicted simultaneously on multiple components.

NAT'L RESEARCH COUNCIL, *supra* note 19, at 1.

94. SIRTF REPORT, *supra* note 13, at 2.

priority customers with limited resources.[95] The SIRTF Report provides recommendations and suggestions for BPS companies to consider as guidance to assist them in developing "their own approaches and flexible plans that would be applicable under a wide variety of circumstances" in the post-Severe Event period or New Normal of degraded service and limited resources.[96] An important characteristic of the New Normal period is that BPS companies would not operate as part of a "large interconnected (and therefore more stable) grid[;]" instead, operators would need to prepare to "manage a number of small electrical islands and implement load shedding or rotating blackouts for extended periods of time (weeks, months or years)."[97] Although "island operation" is not new for BPS companies—and in fact, the BPS itself consists of four large "islands" referred to as "Interconnections"[98]—the post-Severe Event situation would go beyond anything BPS companies had experienced or to date have planned to handle:

> [T]he islands will be much smaller, more numerous, may comprise areas that fall under the authority of several different operating entities, and last for significantly longer periods of time (weeks, months or years) than previously experienced . . . .
>
> . . . Rotating blackouts help manage the supply and demand balance by rotating supply to different blocks of load, typically on a geographic basis, on a defined schedule or timeline.
>
> . . . Following a Severe Event, it is not possible to predict what islands will be formed and this is further complicated when these island boundaries cross the balancing areas that are very familiar during normal operation. In fact, this occurred following the August 14, 2003 blackout . . . .[99]

95. *Id.*

96. *Id.*

97. *Id.* at 3.

98. *Id.* at 18.

99. *Id.* As the SIRTF Report emphasizes, even the August 2003 blackout, by definition, was within the operating experience of the BPS. By contrast, the SIRTF Report points out, "The SIRTF [Report] uses the term 'New Normal' to describe degraded planning and operating conditions *unlike anything the industry has ever*

The NERC Task Forces, however, do not view the August 14, 2003, blackout as providing the kind of experience from which BPS owners and operators can merely extrapolate in order to make plans and preparations for a Severe Event. The August 2003 blackout lasted only a few days; did not damage long lead-time equipment; did not involve an ongoing coordinated, adaptive attack that disrupted internal BPS company communications (or

experienced in North America that could exist for months or years." *Id.* at 14 (emphasis added).

The similarity of certain aspects of operations does not equate with creating something the industry has experienced before because the magnitude of disruption, extent of confusion, and duration of degraded operations remove operations and operators far from what they can extrapolate from in their experiences of previous outages. As the SIRTF Report carefully explains,

> [m]any aspects of operations in the New Normal are not entirely different from what entities have experienced to date but will be much more challenging for a number of reasons. For example, island operation in itself is nothing new—the North American grid is operated in four large islands known as the Interconnections. The challenge in operating islands following a Severe Event scenario is that the islands will be much smaller, more numerous, may comprise areas that fall under the authority of several different operating entities, and last for significantly longer periods of time (weeks, months or years) than previously experienced. Load shedding activities are also likely to be similar to, and very likely based upon, existing load shedding and rotating blackout plans required to respond to EEA-3 conditions (interruption of firm load). However, experience with implementing load shedding plans has been limited to relatively short periods of time—a few hours or at most a day or two. In contrast, under Severe Event conditions, rotating blackouts may need to be implemented for an extended period of time and for significantly longer rotation intervals.
>
> Following a Severe Event on the BPS entities should expect that it will not be possible to fully restore the BPS to pre-event conditions and the system will be significantly degraded. In order to operate the BPS it will likely be necessary to operate in multiple electrical islands, and use emergency criteria, rotating blackouts, and a number of independent control actions to maintain the supply and demand balance and manage frequency and voltage. Rotating blackouts help manage the supply and demand balance by rotating supply to different blocks of load, typically on a geographic basis, on a defined schedule or timeline.

Id. at 18 (footnotes omitted). "The New Normal operating environment may require system operators to operate with far more risk of potentially damaging equipment and/or cascading islands." *Id.* at 33.

communications between BPS companies); and did not involve the generation by malware of false and misleading system status information to operators to deprive them of situational awareness. For such reasons, the August 2003 blackout does not rise to the magnitude of disruption and damage that would qualify an incident as a Severe Event.

The NERC Task Forces carefully define and use the term Severe Event. The term should not become a synonym for a kinetic cyber attack or other disruptive cause that permits a restoration of pre-event levels of BPS operations and services as occurred shortly after the August 14, 2003 outage or after Hurricane Sandy in 2012 (where most BPS customers had power restored by early December—less than six weeks after Hurricane Sandy struck). A better example of a Severe Event (not caused by a cyber attack) was the combination of the earthquake and tsunami that caused the long-term consequences at Fukushima, and which exceeded decades of experiences by Japanese critical infrastructure operators and have continued to date (and thus years later) to overwhelm the recovery efforts.[100]

100. Among the continuing unsolved consequences are that as of August 2013, more than two years after the tsunami initially exposed the local environment to radiation from the Fukushima Daiichi nuclear plant,

> radioactive water is still leaking into the ocean, spelling more trouble for the local fishing industry along the coast of Fukushima prefecture.
>
> Last month the plant's owner, Tepco, finally admitted what many had suspected—that the plant was leaking. Now Japan's Nuclear Regulatory Authority is calling the situation an emergency, and says Tepco's plans to stop the leak are unlikely to work.

Michael Marshall, *Fukushima Leaks Will Keep Fisheries Closed*, NEW SCIENTIST, Aug. 10, 2013, at 01, *available at* 2013 WLNR 19567859.

The use of the word "leak," in such reportage, minimizes and trivializes the ongoing contamination. "Leak" suggests something diminutive (as in "a faucet leak" or "roof leak"). In fact, the "leak" admitted by Tepco on October 1, 2013, turned out to be "four tonnes of rainwater contaminated with low levels of radiation." *Fukushima Plant Operator Reports New Leak*, HUFFINGTON POST (Oct. 1, 2013, 3:29 AM), http://www.huffingtonpost.com/2013/10/01/fukushima-leak_n_4020972.html.

Moreover, NERC's concept of high-impact, low-frequency events has gained recognition by other organizations attempting to prepare critical infrastructure for incidents that far exceed previous experience, surpass what emergency plans had contemplated, and stress all efforts at recovery and restoration of operations and

There are several major causes for the prolonged New Normal period, including:

- if the cyber attack caused overvoltage conditions (as occurred during the geomagnetic disturbance in North America on March 13–14, 1989), generator step-up transformers, among other equipment, could be damaged;[101]
- if such damage is widespread, it could deplete the inventory of spare units and parts that BPS companies maintain;
- if several kinds of heavy equipment, such as transformers, are no longer manufactured in the United States and would have

services. See, for example, the observation by a recent report from *The Chatham House*:

> The frequency of 'high-impact, low-probability' (HILP) events in the last decade signals the emergence of a new 'normal.' Apparent one-off high-profile crises such as 9/11, Hurricane Katrina, the Macondo oil spill and the Japanese earthquake and tsunami were all mega-disasters requiring rapid responses at a global level, marking the beginning of a crisis trend. But lower-profile, persistent events such as flooding, droughts, and cyclones have been shown to have equally serious impacts, raising new questions about the way in which we perceive risk and prepare for disruptive events.
>
> . . . .
>
> Despite considerable efforts to improve scientific understanding and reform risk management approaches, governments and business remain insufficiently prepared to confront HILP crises and effectively manage their economic, social, political and humanitarian consequences.
>
> Current contingency planning often assumes the return of the *status quo ante* after a crisis. But this approach may be inadequate in a world of complex economic and social risks, especially when combined with slow-motion crises like climate change and water scarcity. Slow-motion crises such as these build over many years, but are likely to result in a higher frequency and greater severity of shocks.

BERNICE LEE ET AL., ROYAL INST. OF INT'L AFFAIRS, PREPARING FOR HIGH-IMPACT, LOW-PROBABILITY EVENTS 2 (2012), *available at* http://www.chathamhouse.org/sites/default/files/public/Research/Energy,%20Environment%20and%20Development/r0112_highimpact.pdf.

101. Two such transformers were damaged as a result of the large impulse that occurred in the earth's geomagnetic field along the U.S./Canadian border early on March 13, 1989, and the resulting collapse of the Quebec Interconnection (which started a mere ninety-two seconds after the impulse). *See* Gerry Cauley, *Electric Infrastructure Security Summit: Industry Perspectives Panel*, N. AM. ELECTRIC RELIABILITY CORP. 2 (Apr. 12, 2011), http://www.nerc.com/news/testimony/Testimony%20and%20Speeches/EISS_Cauley_12APR11.pdf.

> to be procured from Asia, the lead times from order to delivery may exceed six months or longer.[102]

102. *See* N. AM. ELECTRIC RELIABILITY CORP., INDUSTRY ADVISORY: PREPARING FOR GEO-MAGNETIC DISTURBANCES 5–6 (2011), *available at* http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2011-05-10-01_GMD_FINAL.pdf (containing recommendations that include: "Inventory assessment: Due to their long-lead manufacture time, identify those installed high voltage transformers . . . that could be damaged from high levels of GIC [geomagnetically induced currents].").

The length of the long lead times for damaged BPS equipment is summarized in a report by the Electromagnetic Pulse (EMP) Commission from 2008, and the facts set forth appear to continue to be an accurate assessment of the acquisition times:

> Recovery from transmission system damage and power plant damage will be impeded primarily by the manufacture and delivery of long lead-time components. Delivery time for a single, large transformer today is typically one to two years and some very large special transformers, critical to the system, are even longer. There are roughly 2,000 transformers in use in the transmission system today at 345 kV and above with many more at lesser voltages that are only slightly less critical. No transformers above 100 kV are produced in the United States any longer. The current U.S. replacement rate for the 345 kV and higher voltage units is 10 per year; worldwide production capacity of these units is less than 100 per year. Spare transformers are available in some areas and systems, but because of the unique requirements of each transformer, there are no standard spares. The spares also are owned by individual utilities and not generally available to others due to the risk over the long lead time if they are being used. Transformers that will cover several options are very expensive and are both large and hard to move.

EMP COMM'N, REPORT OF THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE (EMP) ATTACK 49 (2008), *available at* http://www.empcommission.org/docs/A2473-EMP_Commission.pdf.

Even if such equipment were only partially damaged by a kinetic cyber attack, there would be a prolonged period for restoration of service because the equipment would need to be tested before being returned to service. As the EMP Commission's report explained:

> Even if partially disabled control systems successfully protect the critical generating equipment, all affected plants would face a long process of testing and repairing control, protective, and sensor systems. Protective and safety systems have to be carefully checked out before start up or greater loss might occur. Repair of furnaces, boilers, turbines, blades, bearings, and other heavy high-value and long lead-time equipment would be limited by production and transportation availability once at-site spares are exhausted. While some spare components are at each site and sometimes in spare parts pools

The initial challenge after what appears to be the end of the cyber attack might be that the attack is not singular, that only the first stage has ended, and that subsequent stages may further damage equipment, compromise situational awareness with misinformation displayed to operators, and create confusion and fatigue that leads operators to make more errors and gradually become less capable of handling the multiple crises.[103] As explained in the CATF Report:

> During a cyber attack and the following aftermath, responders may be lulled into the false sense of security that there is only one wave of assault. As with a storm, once the storm passes, everyone pitches in to begin the restoration process with a clear and understood recovery plan. If the attack vector(s) and techniques/tools for the attack are not fully understood and mitigated, the attacker could launch subsequent attacks to disrupt recovery efforts or respond to mitigation efforts. These later attack waves may hold devastating impact potential if not understood and expected.[104]

In order for a BPS company's operations to survive and to be available for the highest priority customers (including hospitals, telecommunications, first responders, and service stations), the owners and operators would need to have planned for isolation of service in "islands" of electric power and to manage for an extended time with degradation of reliable operations. This would "result[] in the gradual reduction in services and functions until essential operations are no longer possible. The key is trying to maintain reliable operations in a reduced state for as long as

> domestically, these would not cover very large high-value items in most cases, so external sources would be needed. Often supply from an external source can take many weeks or several months in the best of times, if only one plant is seeking repair, and sometimes a year or more. With multiple plants affected at the same time, let alone considering infrastructure impediments, restoration time would certainly become protracted.

Id. at 31. We doubt that most critical infrastructure owners and operators have plans for Severe Events, and if they do not, then they probably also have not included in contingency plans an expectation for a prolonged New Normal period and the extent to which that may vary as a result of these extraordinarily long lead times to acquire replacement parts and equipment.

103. *See* CATF REPORT, *supra* note 13, at 29.

104. *Id.*

possible. This resilience characteristic is known as *graceful degradation of service*."[105] In such circumstances, monitoring and situational awareness would decline as "automated processes designed to inform operational staff are systemically severed."[106] Communications between neighboring system control centers would deteriorate and could pose hazards to one another via their communications links as a result of "[i]nternal data corruption, man in the middle scenarios, [and] malicious code injections."[107]

The SIRTF Report identified operational problems that BPS companies would experience during the post-event New Normal, presenting an inexorably complicated situation.

> - Although power is reliably restored to some consumers, planned and unplanned rotating blackouts disrupt service without warning as system operators manage BPS reliability with limited generation and transmission resources and unfamiliar operating conditions.
>
> . . . .
>
> - Other critical infrastructures are affected by electricity disruptions. For example, gasoline and diesel fuel shortages will occur as oil refineries take several days or longer to recover from each electricity service disruption.
>
> . . . .
>
> - Consumers experience large fluctuations in voltage and frequency that may trip sensitive electronic equipment.[108]

What emerges from the SIRTF Report is a cold, hard look at what the BPS could be reduced to following a Severe Event involving a coordinated, sequential, and adaptive cyber attack. The SIRTF Report carefully distinguishes its use of the term "rapid" recovery from its colloquial usage in other critical infrastructure sectors, noting that "'[r]apid' recovery as used by the SIRTF [Report] does not mean rapid recovery to the pre-crisis operation level but to the New Normal."[109] The ensuing prolonged New

105. *Id.* at 28 (emphasis added).
106. *Id.*
107. *Id.*
108. SIRTF REPORT, *supra* note 13, at 16.
109. *Id.* at 13 n.17.

Normal period[110] would ration electricity along what would appear to be an archipelago of electric "islands." Keeping each of those "islands" operational and preventing each from tripping outages in any of the others to which it might still or eventually be interconnected would be challenging for BPS companies. Customary maintenance and repair would become extraordinary because so much would be unfamiliar, resources would be depleted and not quickly or cost-effectively replenished, and the BPS would be operated in a continuously stressed condition.[111] As the SIRTF Report describes it:

> A highly stressed system should be expected during the New Normal period, characterized by islanded operation, rotating blackouts, lower system inertia and higher network impedance (i.e., reduced synchronizing torque), different short circuit currents and critical clearing times, and reduced stability margins. Through the New Normal, protection relay settings may not be optimal and unwanted operations may occur.[112]

Because the SIRTF Report's audience is the BPS operators and owners, it does not address (except in an occasional sentence) the significance of Severe Events for other critical infrastructure companies outside the electric power industry.[113] Instead, the Report focuses its recommendations on helping BPS companies prepare to respond to a Severe Event and to maintain and restore service during the anticipated prolonged New Normal period.[114]

110. *See id.* at 57.

111. *Id.*

112. *Id.*

113. *Id.* at 10–11.

114. The SIRTF Report places primary emphasis on planning and doing so in an evolutionary way throughout the crisis: "The tasks of system planners will evolve through the mitigation, restoration, and New Normal phases of a Severe Event." *Id.* at 47.

> A highly stressed system should be expected during the New Normal period, characterized by islanded operation, rotating blackouts, lower system inertia and higher network impedance (i.e., reduced synchronizing torque), different short circuit currents and critical clearing times, and reduced stability margins. Through the New Normal, protection relay settings may not be optimal and unwanted operations may occur.

Id. at 57.

> By [the return to Normal Reliability] the restoration of system

Thus, the SIRTF Report's suggestions "are in the form of industry guidelines that describe practices that may be used by individual entities according to local circumstances" and are not intended to be adopted or proposed as cybersecurity standards or as a supplement to NERC's cybersecurity CIP Standards.[115] However, the CATF Report and the SIRTF Report continue the approach adopted in the High-Impact, Low-Frequency Report by focusing on *preparations* that companies should make in order to put their personnel in a position to handle post-attack consequences for which they have no previous experience, that existing contingency plans do not address or contemplate, and that the success in handling will therefore depend on the extent to which senior management was willing to extend its previous understanding of what constituted a "worst case scenario" and to make preparations accordingly.[116]

Interestingly, the NERC approach to such situations resembles that of the U.S. Navy's handling of "damage control" for onboard incidents that threaten lives and the integrity of the ship or boat.[117]

> planning capabilities will be complete, although it may differ from the original. System planning efforts may be required to reconcile short and longer-term plans with the requirements of the post-New Normal system and its remaining loads. . . . Factors may include: Permanent loss of load, in particular, industrial load . . . .

Id. at 50.

115. *Id.* at 2.

116. *Id.* at 47–48; CATF REPORT, *supra* note 13, at 1–2, 12–13.

117. NERC's SIRTF Report attempts to prepare owners and operators of BPS companies for being thrust into Severe Events that take them beyond any crisis they or the industry has previously experienced—and to place the emphasis on rigorous, serious preparations, not mere compliance with a minimal standard. The Navy emphasizes such preparations not only through its damage control training, but through the ship integrity checks it routinely conducts. A vivid example, which occurs on surface ships and submarines, is a compartment test for "leaks"—to ensure that each compartment is, indeed, watertight. Notice the Navy's requirements for such tests—and the ultimate use of something as simple, reliable, and available as a "lighted candle" during such checks, which one of the authors of this essay has observed on board a submarine before submerging. The test starts with sealing it and then evacuating the air:

> While the compartment is under test, leaks will be disclosed by hissing or whistling noises as the air escapes. All leaks should be located, marked, and listed for corrective action. You should repair all leaks that were found and then test the compartment again. If the allowable pressure drop is again exceeded on this test, apply a soap

The Navy trains its officers and crews to recognize that the initial response to dangerous incidents, such as onboard fires, hull breaches, and compartment flooding, will probably be the single most important influence on whether the response is ultimately successful.[118] The Navy thus trains in "damage control" by not only simulating the worst-case accidents, but making unavailable certain key personnel so that crews learn to respond to an incident correctly at the start even if the key officers and non-commissioned officers (NCOs) are not present or too injured to give orders and supervise efforts.[119] Similarly, the High-Impact, Low-Frequency Report emphasized:

> solution to the boundaries of the compartment and to all joints, fittings, and closures. When the air pressure is applied, bubbles will be formed by escaping air, thus indicating the location of the leaks.
>
> The observer inside the compartment will have a lighted candle. As the observer goes over areas where leaks are suspected, the deflection of the flame will indicate the location of leaks.

U.S. NAVY, DAMAGE CONTROLMAN: NAVEDTRA 14057, at 3-23 (2003), *available at* http://www.everyspec.com/USN/NAVEDTRA/download.php?spec=NAVEDTRA_14057_AUG2003.018403.PDF.

118. Edward H. Lundquist, *Damage Control Training Makes Sailors Feel the Heat*, DEF. MEDIA NETWORK, (June 18, 2012), http://www.defensemedianetwork.com/stories/sailors-feel-the-heat-2/ ("A crew must be trained to do the right thing, and do it quickly. Thorough and realistic training can truly save lives, and the ship, especially before the extent of the damage gets out of control. According to a World War II Navy manual, *The Handbook of Damage Control*, published by the Naval Damage Control Training Center, Philadelphia in May 1945, '[i]f the ship does not sink within a very few minutes after damage, she probably will survive for several hours.'").

119. On board ship, the term "damage control" does not mean "spin" as in the corporate context. "[D]amage control is serious business and an 'all-hands' responsibility." U.S. NAVY, *supra* note 117, at 1-4. Current damage control procedures, set forth in NTTP 3-20.31 (Surface Ship Survivability), chapter 5, are under restricted access and not available to the general public. Our experience in working and speaking with U.S. and foreign navy personnel and navy engineers informs our statements in this section. In addition, passages from U.S. Navy publication *Damage Controlman*, NAVEDTRA 14057, reflect the Navy's view that each member of a damage control party should be capable of acting correctly if orders are not quickly received and capable of taking the place and discharging the responsibilities of other members of the damage control party. Illustrative are the following passages:

> Your ability to lead others is particularly important because in casualty situations damage control often becomes an 'all-hands' evolution. In these situations, a Damage Controlman holds a key position in the

> As HILF [high-impact, low-frequency] risks occur very infrequently, the success or failure of a response is more dependent on *thorough planning and preparation than on operational experience*. The ability to effectively respond to a changing threat environment—especially in the case of an adaptive attack—will be measured by the efficacy of the system operator's *initial response*. The operator will rely on the sophistication of the tools under his immediate control and his training in those circumstances, neither of which can be provided in the minutes preceding an event. These tools and the training needed to ensure an appropriate response must be developed and deployed well in advance of the event.[120]

In short, the focus of the NERC Task Force reports is on *preparedness* for infrequent, unprecedented Severe Events and the resulting New Normal conditions. Those conditions of uncertainty, stress, and impaired situational awareness and the challenges requiring a resourceful response cannot be adequately handled with "last minute" preparations or plans that have been rehearsed under good conditions instead of those that stress their underlying assumptions.

> damage control organization and is required to coordinate the efforts of others for the successful control of damage.
>
> . . . .
>
> . . . [E]ach repair party needs to monitor the reports from all the other repair parties. By monitoring these reports, each repair party will be able to assume the duties of DCC [the damage control center] if DCC becomes a battle casualty.
>
> . . . .
>
> Provide for a repair party, remotely located from DCC [the damage control center], to assume the responsibilities of DCC, in the event that DCC becomes a battle casualty.
>
> . . . .
>
> No two emergency situations are identical. Therefore, the corrective action taken will vary to some extent. The responsibilities of each member of the fire party will normally remain the same. However, there are times when a person will have to assume other responsibilities. As an example, the nozzleman is injured while fighting a fire. The hoseman then takes the nozzleman's place. The nozzleman is evacuated from the scene and another person replaces the hoseman.

Id. at 1-1, 2-2, 2-8 to -9, 2-11.

120. HILF REPORT, *supra* note 13, at 23.

If the White House initiatives and NERC initiatives were both directed at addressing cyber attacks that might cause a Severe Event, then their respective recommendations to critical infrastructure companies might be creating a coherent plan of action for such companies and their operators and owners. Instead, as we explain in the next section, the White House initiatives do not expressly reflect the findings of NERC's CATF Report and SIRTF Report, nor do they view a Severe Event as a definitive worst-case scenario or contain any recommendations or directions that would do much to urge critical infrastructure to prepare to address such a degradation of services. In short, although the White House initiatives speak in terms of "catastrophic" consequences, those initiatives have much lower objectives, and achievement of them would appear to do little to protect critical infrastructure against the consequences of a Severe Event.

G. Cyber Threats as Envisioned by Executive Order 13636, PPD-21, and Explanations by White House Staff

Although the EO cites "[r]epeated cyber intrusions into critical infrastructure" and characterizes their occurrence as "one of the most serious national security challenges,"[121] the EO only gives a hint about the consequences of such intrusions.[122] The hint consists simply of the EO assertion that certain critical infrastructure, if affected by a "cybersecurity incident," could result in "catastrophic regional or national effects."[123] The EO, moreover, does not use cyber-threat terms, such as "coordinated cyber attack," "severe impact," "Severe Event," or "New Normal," adopted by the NERC Task Force reports, which were issued nine months earlier and thus available to the White House drafting team.[124]

121. Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,739 (Feb. 19, 2013).

122. Moreover, the term "intrusions" does not equate with "attacks" and often intelligence-gathering "intrusions" precede the launch of a cyber attack. Thus, it is unclear from the EO what percentage of such "intrusions" are attacks and which kinds of "intrusions" the EO seeks to address and might assign the highest priority to averting.

123. 78 Fed. Reg. at 11,742.

124. The EO also does not use any of the supplemental terminology that the SIRTF Report adopts for discussing "resilience" of the BPS, such as "robustness" ("[t]he ability to absorb shocks and keep operating"), "resourcefulness" ("[t]he ability to manage a disruption as it unfolds"), and "rapid recovery" ("[t]he ability

We received an advanced copy of the EO, read those words early that evening, and anticipated that the President would draw attention to and express the gravity of that threat in his State of the Union address, which he was to deliver that night. Instead, he mentioned the threat and the EO in passing, treating it as just another item on a State of the Union checklist. The President described it in terms that minimized and trivialized the threat (words that we put in italics) in the following text of the President's address:

> America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and *infiltrate private e-mail*. We know foreign countries and companies *swipe our corporate secrets*. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of *real threats* to our security and our economy.
>
> And that's why, earlier today, I signed a new executive order that will strengthen our cyber defenses by increasing information sharing, and developing standards to protect our national security, our jobs, and our privacy.[125]

The President's State of the Union address made cyber threats to the nation's critical infrastructure seem anything but urgent or imminent. And more surprisingly, the President made the threat and the response to it appear neat, clean, clear, and straightforward. However, to owners and operators of critical infrastructure companies, the cyber threats targeting their enterprises and the allocation of responsibilities for addressing those threats appear quite different—complicated, messy,[126] murky, and disorienting. Operators and owners of critical infrastructure

to get back to [n]ormal as quickly as possible"). *See* SIRTF REPORT, *supra* note 13, at 102.

125. Barack Obama, President of the U.S., State of the Union Address (Feb. 12, 2013) (transcript available at http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address) (emphasis added).

126. T.E. Lawrence observed: "Analogy in human things was fudge, anyhow; and war upon rebellion was messy and slow, like eating soup with a knife." SEVEN PILLARS OF WISDOM: A TRIUMPH 193 (1935). Cyber war too is "messy" and slow only in the preparation, not in the execution.

companies—and their companies' boards of directors—were left asking just how "credible" is the cyber threat if the President describes it with no sense of urgency, no sound of alarm, and no clear statement of the actions the federal government will take to address it.

Moreover, the conclusory assertion that the nation's cyber defenses would be strengthened by "increasing information sharing [with private industry]" may have been puzzling to owners and operators of BPS companies who may have recalled that a few months earlier FERC Chairman Wellinghoff made "information sharing" appear of limited, if any, use to a cyber-targeted BPS company. As Chairman Wellinghoff put it, "If I had a cyber threat that was revealed to me in a letter tomorrow, there is little I could do the next day to ensure that that threat was mitigated effectively by the utilities that were targeted."[127]

Owners and operators of BPS companies and their boards of directors cannot ignore or fail to prepare for federal information sharing that might put them on notice of imminent cyber threats against their enterprises. Moreover, as PPD-21 (issued that same night) makes clear, the White House views the owners and operators of critical infrastructure as ultimately responsible for the cybersecurity of their enterprise and, in some mysterious, unexplained way, for integrating their preparations with the "national preparedness system." As PPD-21 states in its introduction:

> Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.
>
> Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.[128]

PPD-21 purports to establish national policy on "critical infrastructure security and resilience."[129] Inexplicably, for two key policy directives originating in the White House on the same day,

127. Colman, *supra* note 33.
128. PPD-21, *supra* note 38, at 1.
129. *Id.*

PPD-21 emphasizes a concept—"resilience"—that appears only once in the EO.[130] The term "resilience" appears forty-four times in PPD-21, which defines it to mean

> the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.[131]

Throughout PPD-21 the term "security" tends to be paired with "resilience" (e.g., "security and resilience")[132] suggesting that while the EO aims more at protecting critical infrastructure from an attack, PPD-21 aims at defense and also at withstanding an attack and post-attack recovery. However, PPD-21's use of "resilience" consistently denotes a capability to "recover rapidly" from cyber attacks, without drawing any distinction between the severities of such attacks.[133] As a result, the federal government personnel who read PPD-21 will not be encouraged by its text to consider Severe Event consequences of the kind identified by the NERC Task Force reports. They will not be contemplating or attempting to prepare for incidents whose causes and consequences extend beyond previous experience and create a prolonged New Normal period of reduced levels of service. Nor will they feel the need to prepare to mitigate the damage in the orderly manner recommended by the NERC Task Force reports, in essence, preparing to manage a "graceful degradation" of the BPS and related services.

Equally important, while the NERC Task Force reports make clear their recommendations are for voluntary adoption and implementation by the private industry owners and operators of the BPS and thus are private industry *responsibilities*,[134] the EO and

130. Compare *id.*, which references "resilience" forty-four times (including the title), with Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11, 739 (Feb. 19, 2013), which only refers to "resilience" in section 1.

131. PPD-21, *supra* note 38, at 12.

132. The phrase "security and resilience" appears forty-two times in PPD-21. *See id.*

133. *Id.*

134. *Compare* CATF REPORT, *supra* note 13, *and* SIRTF REPORT, *supra* note 13, at 10, 7 ("This report addresses important aspects related to enhancing the resilience of the bulk power system in the face of a Severe Event. It provides entities with practical options to enhance their capabilities to prepare, mitigate

PPD-21 speak repeatedly and ambiguously of government and private industry sharing responsibilities without making very clear how owners and operators of critical infrastructure will know which responsibilities are the government's and which are private industry's.[135] For example, PPD-21 asserts a defense and rapid recovery objective and then identifies all the potentially responsible parties under the ambiguous rubric—"shared endeavor responsibility"—without drawing lines to distinguish one party's responsibilities from another's:

> Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards . . . .[136]
>
> This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a *shared responsibility* among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as "critical infrastructure owners and operators").[137]

and restore the operation of the bulk power system."), *with* PPD-21, *supra* note 38, at 1 ("The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.").

Compare the options considered and "Key Recommendations" set forth in CATF REPORT, *supra* note 13, and SIRTF Report, *supra* note 13, at 7 ("suggestions offered . . . are intended to prompt entities to develop their own approaches and flexible plans that would be applicable under a wide variety of circumstances"), with PPD-21, *supra* note 38, at 1 ("[Critical infrastructure security and resilience] is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure.").

135. *See* Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,739 (Feb. 19, 2013); PPD-21, *supra* note 38, at 1 ("This endeavor is *a shared responsibility* . . . .") (emphasis added).

136. PPD-21, *supra* note 38, at 1. Note the unadmitted or unwitting internal contradiction in that sentence. If critical infrastructure is "secure and able to withstand . . . all hazards," then the ability to "rapidly recover from all hazards" would not be a necessary and equal objective. The more one reads such sentences, the more they appear to gloss over the harsh realities of a damaging cyber attack and to posit objectives as if the language of asserting them also achieved them—a kind of "mission accomplished" by "mission defined" assertion.

137. PPD-21, *supra* note 38, at 1 (emphasis added).

The ambiguous boundary lines of responsibility for "security and resilience" become even murkier and harder to distinguish when PPD-21 proceeds to make vacuous statements asserting that things will happen that no one could intelligently identify, quantify, or observe.[138] For example: "The Federal Government also has a responsibility . . . to organize itself to *partner effectively with* and *add value to* the security and resilience efforts of critical infrastructure owners and operators."[139] The verb "to partner" suggests an equality between parties, which clearly does not exist between the federal government and "owners and operators of critical infrastructure" and is thus both ambiguous and misleading. The verbal phrase "add value" is worse because it suggests the adding of a non-existent and unquantifiable "value" to "security and resilience efforts," which is clearly not intended as monetary, financial, or marketable and comes across as mere bureaucratic puffery.[140] When trying to

138. Such broad PPD-21 statements include: "Critical infrastructure must be secure and able to withstand and rapidly recover from *all hazards*. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery." *Id.* (emphasis added).

139. *Id.* (emphasis added).

140. The federal government's offer of adding "value" to the private efforts of critical infrastructure owners and operators in this context essentially means the federal government is offering to add the heft, might, and law enforcement powers of the government, not financial or monetary value. The authors are aware, however, from confidential interviews with critical infrastructure owners and operators, that during heightened security events, such as major public gatherings that have occurred for national events, law enforcement, and Homeland Security officials have installed computer tools and software on local IT infrastructure deemed to be particularly temporarily vulnerable to a cyber attack. While the private critical infrastructure operators appreciated federal offers of resources and assistance, the resources are perceived to be of limited value in part because they are the IT equivalent of sharing a "no fly list" with the pilots of an aircraft. A tool aiding in spotting past bad actors of cyber incidents offers little comfort of spotting a future bad actor. Furthermore, providing the federal government with access to help a critical infrastructure operator means potentially breaching (1) confidentiality obligations with respect to personally identifiable customer information by opening private computer systems to federal government screening and surveillance tools, and (2) NERC's Critical Infrastructure Protection standards by allowing unauthorized persons with access to critical infrastructure. In fact, the NERC SIRTF Report contemplated that a critical infrastructure operator may be forced into a "Hobson's Choice" at times by needing to violate certain NERC Critical Infrastructure Protection standards in responding to a Severe Event: "Although a Severe Event may put entities in a position where they cannot comply with all standards, entities are in the best position to 'do the right

summon private industry to work with the federal government to meet a national security challenge, it is rarely helpful to address owners and operators of critical infrastructure in terms that they will not understand, will find devoid of meaning, and will therefore have good reason to infer may have been drafted with serious intent but without rigorous and serious thought.

PPD-21 includes other examples of policy platitudes, vacuous statements, and internal inconsistencies:

> Although the roles and responsibilities identified in this directive are directed at Federal departments and agencies, effective partnerships with critical infrastructure owners and operators . . . are imperative to strengthen the security and resilience of the Nation's critical infrastructure.[141]
>
> . . . .
>
> An effective national effort to strengthen critical infrastructure security and resilience must be guided by a national plan that identifies roles and responsibilities and is informed by . . . capabilities . . . and responsibilities of . . . Federal departments and agencies with critical infrastructure roles . . . and critical infrastructure owners and operators.[142]

Any time a directive states that an "effective national effort" must be "guided by a national plan that identifies . . . responsibilities" and that is "informed by . . . responsibilities," the effort at reasoning has become painfully circular and unhelpful, if not counterproductive, to its audience of federal personnel and owners and operators of critical infrastructure.

As a result, what can boards and management of critical infrastructure draw from the EO and PPD-21 regarding the nature of the cyber threat to their enterprises? Nothing definitive can be drawn, we submit, beyond the fact that the "repeated intrusions"[143]

thing' for reliability and public safety, and self-report any violation of NERC standards as time and circumstances permit." SIRTF REPORT, *supra* note 13, at 8, 10, 17.

141. PPD-21, *supra* note 38, at 2.

142. *Id.* at 5–7.

143. Although not described in the EO or PPD-21, boards and management of critical infrastructure companies, known as DHS's ICS-CERT, reported in July 2013 that cybersecurity attacks on the energy sector continue to outpace attacks on

pose a "national security" challenge and that both the federal government and private industry have responsibilities that remain, for private industry, ill defined.

What do the EO and PPD-21 tell boards and management about the White House objectives for improving critical infrastructure cybersecurity? Again, critical infrastructure companies can infer very little, except that the objectives appear not to address Severe Events, managing "graceful degradation" during and after them, and the resulting consequences of a prolonged New Normal of reduced levels of services.[144]

The wide divergence between the objectives of the White House initiatives and those of NERC's CATF and SIRTF Reports becomes clearest when one reviews the explanation of the EO's objectives by the White House Senior Director for Cybersecurity, Andy Ozment:

> The main [cybersecurity] problem is advanced persistent threats ["APTs"]—cyber hygiene will not protect you from APTs. The adversaries' use of APTs is their "A-Game"—but the adversaries are not using their A-Game. They don't need to. But if we can force them to focus on their A-Game, we can focus our resources on defeating that. So we want to raise the water level for all companies' cybersecurity.[145]

Boards and management of critical infrastructure companies therefore must decide how their companies will respond to the White House's cybersecurity objectives and measures to achieve them, detailed by the EO, and NERC's cybersecurity objectives and

all other critical infrastructure sectors, with fifty-three percent or 111 confirmed cyber attacks occurring on the energy sector. *See Brute Force Attacks on Internet-Facing Control Systems*, ICS-MONITOR (U.S. Dep't of Homeland Sec., Wash., D.C.), Apr./May/June 2013, at 2, *available at* http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf.

144. See SIRTF REPORT, *supra* note 13, at 2, 10, for discussions of Severe Events and New Normal and CATF REPORT, *supra* note 13, at 10, 27, for discussion of "graceful degradations." These concepts are not discussed in the EO or PPD-21.

145. Andy Ozment, Senior Dir. Cybersecurity, White House, Fifteen Years of Being Nervous: Security U.S. Critical Infrastructure, Address Before RSA Conference 2013 (Feb. 28, 2013) (notes on file with author) (quotation based on notes taken by author Roland Trope, who was in the audience for Mr. Ozment's talk).

measures to achieve them, set forth in the CATF and SIRTF Reports.

In the previous sections, we highlighted the differences between the CATF and SIRTF Reports' objectives and the EO's objectives. In the next two sections, we review their substantially different approaches and measures for achieving their respective objectives and the cybersecurity choices they present to boards and management of critical infrastructure companies.

V. CYBERSECURITY STRATEGIES OF EXECUTIVE ORDER 13636

In this section, we highlight the EO's objectives and its strategies for achieving them. The EO, although directed at federal agencies, is ultimately concerned with, as Mr. Ozment put it, raising the "water level for all companies' cybersecurity."[146] To accomplish that, the EO attempts indirectly to coax companies into making substantial changes in their cybersecurity habits by two fundamental strategies: one involves increasing the federal government's sharing of cyber intelligence reports with private industry, and the other involves assembling a select set of standards and industry best practices (referred to as the "Cybersecurity Framework") that industry will be encouraged to adopt and comply with voluntarily.

A. Information Sharing

The EO authorizes three kinds of information sharing by the federal government with qualified critical infrastructure companies.

1. Classified Information Shared Through Third-Party Vendors

First, to assist owners and operators of such companies, the EO directed the Secretary of Homeland Security ("DHS Secretary"), in collaboration with the Secretary of Defense, to "establish procedures to expand the Enhanced Cybersecurity Services program" in order to "provide *classified cyber threat and technical information*" to "eligible critical infrastructure companies or

146. *Id.*

commercial service providers that offer security services to critical infrastructure."[147]

As explained by the White House, this kind of *classified* information sharing would actually be indirect: DHS would give the classified information to qualified (government contract) vendors with the capability to store and protect it, and they in turn would release it, for a fee and under protective conditions, to eligible critical infrastructure companies.[148] The information would consist of "classified signatures . . . to block malicious traffic."[149] The White House justification for releasing only this limited scope of threat information is that to release more sensitive information would only cause the adversaries to respond rapidly and change the attack vectors and other behavior, which companies would then again have to detect and attempt to thwart.[150]

By early August 2013, DHS had approved only two vendors and vetted seven companies to participate in the program, but they "haven't gone live yet."[151] Boards and management might find serious drawbacks to this offer of information sharing. The vendor intermediaries would be in a position to filter what information or portion of information they sold and perhaps to sell different portions to different customers. There might also be potentially significant delays in transfer of the information from DHS to the vendor and then on to the critical infrastructure company. It is doubtful to us whether such companies will welcome or find much use for such information by this route, and as of yet at an undetermined price.

147. Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,739 (Feb. 19, 2013) (emphasis added).

148. *See* Joseph Menn, *Government to Share Cyber Security Information with Private Sector*, INS. J. (May 15, 2013), http://www.insurancejournal.com/news/national/2013/05/15/292065.htm.

149. Andy Ozment, Senior Dir. Cybersecurity, White House, Protecting the Electric Grid from Cyber Attacks: Where Do We Stand, Address Before Electric Grid Cyber Security Initiative, (Aug. 6, 2013) (notes of speech available from author), *available at* http://bipartisanpolicy.org/events/2013/08/protecting-electric-grid-cyber-attacks-where-do-we-stand.

150. *See* Menn, *supra* note 148.

151. Ozment, *supra* note 149.

2. High Risk Companies Identified in "Catastrophic Target Notices"

The second kind of information would also appear to be of limited benefit to critical infrastructure company recipients because it will tell them what they already know. The EO authorizes what could be termed "Catastrophic Target Notices." These Notices purportedly attempt to use "consistent, objective criteria" to identify the critical infrastructure at the greatest risk from cyber attack. However, they actually identify critical infrastructure companies that, if damaged by a cyber attack, would cause widespread damage to other companies.[152] The DHS Secretary is to use a "risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[153]

The Notices would also provide recipients with the basis for that determination and give them a "process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration" of their identification.[154]

That the EO would give owners and operators a procedure for, in essence, challenging the identification, strongly suggests that the identification imposes some burdens that owners and operators may prefer to avoid. Being identified could hardly come as a surprise to most critical infrastructure owners and operators. For example, BPS owners and operators know from their experience with outages caused by severe weather that if their ability to provide electric power to their customers substantially declines for even a short period their customers will probably experience damage.[155]

152. *See* Roland L. Trope & Stephen J. Humes, *By Executive Order: Delivery of Cyber Intelligence Imparts Cyber Responsibilities*, IEEE SECURITY & PRIVACY, Mar./Apr. 2013, *available at* http://www.hklaw.com/publications/By-Executive-Order-Delivery-of-Cyber-Intelligence-Imparts-Cyber-Responsibilities-04-01-2013/.

153. Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,742 (Feb. 19, 2013).

154. *Id.* (providing owners and operators of critical infrastructure with an "opt-out" procedure by allowing them to "submit relevant information and request reconsideration of identifications").

155. Energy sector critical infrastructure companies are already subject to NERC's Critical Infrastructure Protection standards, one of which already requires them to characterize their operations and infrastructure to identify assets subject to the reliability standards. *See, e.g.*, *Standard CIP-002-3—Cyber Security—Critical Cyber Asset Identification* 1 (Dec. 16, 2009), *in* BPS RELIABILITY STANDARDS, *supra* note 77.

And the longer it takes to restore full electric power to customers, the greater the damage will likely be to customers. Critical infrastructure owners and operators would probably not succeed in a request to be removed from the group of companies identified by a Catastrophic Target Notice.[156] Something else would appear to have motivated the provision for an opt-out procedure.

We think that there are three plausible reasons that may have motivated the White House to make an opt-out procedure available. First, the White House presumably recognized that delivery of a Catastrophic Target Notice to owners and operators of a company will not be neutral and without significance. On the contrary, receipt of such notice will in all likelihood impose on owners and operators a documented "formal notice" of the identification. Since that Notice will be based on a federal government determination, it will in all likelihood be accorded significant evidentiary weight in lawsuits wherein plaintiffs allege that they would not have suffered damage from a cyber attack against the defendant critical infrastructure company but for the negligent failure of the company to act responsibly after receipt of such notice. In such a lawsuit, recipient owners and operators will

156. NERC will vigorously defend its regulatory reach over any company that is connected electrically to the nation's BPS at greater than 100 kV, whether the entity is a load-serving entity (which directly supplies electricity to end-use customers), distribution provider, wholesale generator, or other transmission owner or operator. NERC's position is based on Rule 501.1.4 of the NERC Rules of Procedure, which provides:

> For all geographical or electrical areas of the Bulk Power System [("BPS")], the Registration process shall ensure that (1) no areas are lacking any entities to perform the duties and tasks identified in and required by the Reliability Standards to the fullest extent practical, and (2) there is no unnecessary duplication of such coverage or of required oversight of such coverage.

N. AM. ELECTRIC RELIABILITY CORP., RULES OF PROCEDURE OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION 46 (2013), *available at* www.nerc.com /FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20131004.pdf. NERC's Compliance Registry lists entities that are subject to, and obligated to comply with, mandatory and enforceable Reliability Standards in accordance with Appendix 5B to the NERC Rules of Procedure. *Id.* NERC recently challenged a FERC order that found a certain company could be removed from its Compliance Registry. *See* S. La. Elec. Coop. Ass'n, 144 FERC ¶ 61,050 (July 18, 2013), *appeal docketed*, No. RC 12-4-000 (FERC Aug. 19, 2013), *available at* http://www.nerc.com /FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Final_Filed_SLECA _Registration_Appeal.pdf.

not be able to argue plausibly that they and their companies did not "foresee" the risks to others of a cyber attack damaging their own operations. And, by definition, the risks extend not only to customers and suppliers, but to a much broader category of "catastrophic regional or national effects on public health or safety, economic security, or national security."[157] Unless the Catastrophic Target Notice specifically limited its scope to one of those potential impacts, then by definition the owner and operator recipients have been "put on notice" that unless they improve their preparations to thwart cyber attacks, mitigate their impacts (including perhaps preparing for a "graceful degradation" of operations), and restore services as soon as practicable, they may not be able to raise a "lack of foreseeability" defense in the event they are sued (by customers, suppliers, and other indirectly damaged critical infrastructure companies) for negligently failing to avert or mitigate such damages.

The second reason is that although an executive order, unlike a federal statute, is not law and cannot impose duties or obligations on any organization or person outside of the executive branch, it can nonetheless impart certain responsibilities by sharing sensitive information that concerns threats and risks to owners and operators of critical infrastructure that the general public does not receive. Recipients cannot simply read such notices, file them in a drawer (or save them to a file), and ignore them. Instead, as we explained in an article shortly after issuance of the EO:

> [R]ecipients [of a Catastrophic Target Notice] must come to terms with the possibility that the DHS has imposed on owners and operators, directors and officers, a set of undefined, ambiguous but possibly extraordinary corporate cyber responsibilities. Imagine a specter of burgeoning liability that could attach to your company or its board if a cyberattack strikes and demonstrates the accuracy of the DHS's warning of catastrophic regional or national damage. Cyber insurance policies might start excluding from coverage recipients of DHS notices or condition coverage on steeply priced premiums.[158]

The third reason derives from the other two: no company will want the burden of being identified by a Catastrophic Target

157. Exec. Order No. 13,636, 78 Fed. Reg. at 11,742.

158. Trope & Humes, *supra* note 152, at 63, 66.

Notice. It's the equivalent of having a bull's-eye placed on the company—making it a target for regulators' scrutiny, post-attack investigations by government entities, and parties seeking to recover damages from the "deep pockets" of a critical infrastructure company. Such a Notice brings no added prestige or reputational boon. Thus, owners and operators of smaller critical infrastructure companies will want, if possible, to avoid identification by a Catastrophic Target Notice. If they receive a Catastrophic Target Notice, they may want to give serious consideration to attempting to persuade DHS to withdraw the Notice, using the appeal of Notice procedure that the EO requires the DHS Secretary to establish for "reconsideration of identifications."[159]

If a company's request for reconsideration of identification is unsuccessful the first year, it may want to attempt again the following year because the EO requires the DHS Secretary to "review and update the list" of companies identified by a Catastrophic Target Notice.[160] Owners and operators of the largest critical infrastructure enterprises who receive such Notices will almost certainly view them as identifying their company as a high-risk target—and presumably a high-value target for a cyber adversary. As a consequence, these owners and operators may perceive (and will have good reason to perceive) that a Notice enhances their responsibility to make preparations to improve the company's resilience, their ability to mitigate damages flowing directly across a region or the nation from any disruption and impairment of the company's services, their capability to manage a "graceful degradation" of such services, and their resourcefulness in handling a prolonged New Normal until full service can be restored.

Our interpretation of the EO's intended purpose for Catastrophic Target Notices is supported by explanations provided by the White House:

> [I]n some places, we want to focus on the most critical of the critical—an elevated threshold—where harm to that infrastructure can cause catastrophic harm regionally or nationally.

159. 78 Fed. Reg. at 11,742.
160. *Id.* § 9(a), at 11,742.

> We are going to be particularly sensitive about *cascading risks and interdependencies of harm* to those who depend on these most critical of the critical infrastructures.
>
> We will confidentially notify you, *then concentrate our out-reach efforts on you. We want to focus our efforts on you—make sure you improve your understanding of the national risk,* and have that baseline to improve the national risk management.[161]

This passage appears to leave little doubt that the White House believes—and will encourage others to believe (be they regulators, commercial parties, judges, or juries)—that receipt of a Catastrophic Target Notice imparts an enhanced set of responsibilities. Not only will such recipients be expected (and told) to improve their "understanding of the national risk," but also, based on that improvement, to implement preparations that reduce that risk.[162] Such an undertaking may impose prodigious costs on the "most critical of critical infrastructure" recipients of these notices. And who will they most likely be? The answer can be derived from Mr. Ozment's reference to "cascading risks"[163] (like cascading outages) and, more definitively, from a passage in PPD-21, which states: "This directive also identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors."[164]

As owners and operators try to make sense of the significance of receiving a Catastrophic Target Notice, they may also ask why the EO expressly exempts a remarkably important sector of critical infrastructure companies from identification by such Notices—even those involved in operating or developing "communications systems" which PPD-21 identified as "uniquely critical" to the cybersecurity of the nation. The EO expresses the exemption as follows: "The Secretary shall not identify any *commercial information*

161. Ozment, *supra* note 145 (emphasis added).

162. 78 Fed. Reg. at 11,742. Risk mitigation is not limited to recipients of catastrophic target notices. Pursuant to section 10(e), even independent federal agencies, such as FERC and the Nuclear Regulatory Commission, are encouraged to "consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities." *Id.* at 11,743.

163. Ozment, *supra* note 145.

164. PPD-21, *supra* note 38, at 2.

technology products or consumer information technology services under this [Catastrophic Target Notice] section."[165]

The EO does not define the terms "commercial information technology products or . . . services,"[166] but it is hard to imagine a definition that would not overlap with an interpretation of the term "communications systems."[167] Moreover, it is reasonable to infer that companies eager to qualify for that exemption will include: developers and providers of software (e.g., Microsoft), internet search engines (e.g., Google), cloud-computing services (e.g., Amazon), smart phone and smart tablets (e.g., Apple), social network services (e.g., Facebook), and short-burst communications (e.g., Twitter). This list could reasonably grow to include most of the major Silicon Valley companies. Exempting these companies from Catastrophic Target Notices seems inexplicable, particularly because many of them are arguably among those most responsible for creating cybersecurity vulnerabilities in critical infrastructure companies that the EO seeks to reduce; many of these Silicon Valley companies have sold products with security deficiencies for decades, but they have seldom been held liable.[168]

The EO gives no justification or rationale for the exemption, and the need for a justification would appear compelling since the EO seeks to address a national security challenge. One suspects that the exemptions reflect successful lobbying by these companies.[169] The apparent desire of information technology

165. Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,742 (Feb. 19, 2013) (emphasis added).

166. *See id.* at 11,742.

167. The phrase "communications systems" is coupled with "energy" twice in PPD-21 as essential for all critical infrastructure sectors. PPD-21, *supra* note 38, at 2, 9.

168. *See* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable* 3 (Univ. of Chi. Inst. For Law & Economics, Working Paper No. 217, 2004), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=573502 (arguing that "ISPs should, to some degree, be held accountable when their subscribers either originate malicious Internet code or propagate that code by, for example, forwarding a virus over email or adopting lax security precautions that in turn allow a computer to be co-opted by a malevolent user").

169. Most likely, the source of the EO's exemption for these commercial information technology companies is an import by the White House from the prior failed legislation, the Cyber Security Act (CSA) of 2012, the so-called Lieberman–Collins bill that failed to pass the Congress in November 2012. *See* Jennifer Martinez & Ramsey Cox, *Senate Votes Down Lieberman, Collins Cybersecurity*

companies to avoid identification with a Catastrophic Target Notice adds further weight to the argument that receipt of such Notices imparts a heavy burden of new corporate cyber responsibilities. Information technology companies appear to have foreseen the risks that notices would create for them and persuaded the White House to add a special exemption just for them. It is, however, the kind of exemption that will strike owners, operators, and boards of other critical infrastructure companies as evidencing a lack of seriousness of purpose in the EO, especially since several of the exempt companies have been among those that have suffered the most significant exfiltrations of valuable data and intellectual property from cyber attacks[170] (e.g., Google).[171]

3. Targeted Companies Identified in "Imminent Target Notices"

The EO's third kind of authorized information sharing imparts an even larger burden of responsibilities to its recipients. In these instances, the EO authorizes the DHS to share federal intelligence about cyber attacks planned against the U.S. homeland whose targets are known or suspected.[172] The notices will omit any classified intelligence from which they derive and will thus be limited in what they tell the recipients, beyond the fact that the recipient company has been identified as one of the planned cyber attack's targets. For that reason, we refer to them as "Imminent

Act a Second Time, THE HILL (Nov. 14, 2013, 11:12 PM), http://thehill.com/blogs/hillicon-valley/technology/268053-senate-rejects-cybersecurity-act-for-second-time. The CSA defined a "commercial information technology product" as "a commercial item that organizes or communicates information electronically." Cybersecurity Act of 2012, S. 2105, 112th Cong. § 2(1) (2012). The failed bill exempted such "commercial information technology products" from regulation as critical infrastructure. *Id.* § 103(b)(2)(C). This exemption included "installation services, maintenance services, repair services, training services, and any other services provided in support of the product." *Id.* § 103(b)(2)(D).

170. *See* GA. INST. OF TECH., EMERGING CYBER THREATS REPORT 2013, at 4 (n.d.), *available at* http://gtsecuritysummit.com/pdf/2013ThreatsReport.pdf. Among others, the report notes a Microsoft vulnerability that allowed hackers to manipulate firmware on a PC until Microsoft released Windows 8 with Secure Boot technology. *See id.* at 5.

171. *See* Matthew Prince, *Post Mortem: Today's Attack; Apparent Google Apps/Gmail Vulnerability; and How to Protect Yourself*, CLOUDFLARE (June 2, 2012, 12:22 AM), http://blog.cloudflare.com/post-mortem-todays-attack-apparent-google-app.

172. Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,739–40 (Feb. 19, 2013).

Target Notices." Unlike the Catastrophic Target Notices, the unclassified versions of these notices can be delivered to companies whether or not they operate critical infrastructure.[173] The EO says little about the substance of these Notices other than that they will be "*unclassified reports* of cyber threats to the U.S. homeland that identify a specific targeted entity."[174]

As the EO describes this more informative type of Imminent Target Notice:

> (a) . . . . Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security . . . , and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order *to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity.*[175]
>
> (b) The [DHS] Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports . . . to the targeted entity.[176]

The EO explains that both the classified and unclassified Notices reflect U.S. policy "to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats."[177]

Since the EO describes the purpose of Imminent Target Notices as enabling recipients to "better protect and defend themselves,"[178] it is reasonable to infer that delivery of such Notices imparts a corporate cyber responsibility to the recipients to make good use of that timely, sensitive information. Boards and management of potential recipients of such Notices will need to

173. *Id.* at 11,739 ("The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations."). Recipients therefore will presumably not receive any information that could reveal anything about the investigations and probably would not identify the source or even the kind or timing of the planned cyber attack.

174. *Id.* (emphasis added).

175. *Id.* (emphasis added).

176. *Id.*

177. *Id.*

178. *Id.*

address to what extent their companies will attempt to fulfill such responsibilities. Such considerations may include the following:

> If you're an owner or operator, a director or officer, and the government alerts you that your company [is] a target, it's probably going to be hard to avoid asking yourself, your executive management team, your board, and your counsel a battery of questions: "We can't ignore this, can we? Does this trigger any disclosure or reporting obligations? Do stockholders have the right to know this company has been identified a target so they can make informed investing decisions? What should we be doing before we're attacked? Shouldn't we reexamine our cyber defenses and disaster recovery plans? If we don't, and we're severely damaged and slow to restore operations (as after super-storm Sandy), it will drive up the recovery costs, tank our reputation, and hammer the company's valuation. If our customers, suppliers, and stockholders learn that we had warning and didn't prepare to limit damage and recover quickly, they'll blame us for their losses—direct or collateral—and they'll sue us."[179]

Perhaps prompted by those and other concerns, directors, management, and their counsel might ask what else these notices will reveal. From the text of the EO and public speeches by White House officials, these Imminent Target Notices will not reveal any of the following concerning the planned cyber attack:

- Originating country or organization, or identity of participants;
- Nature of attack;
- Number and identity of other known "targets" (i.e., Imminent Target Notices will not alert recipients to who else has or will receive such Notice);
- Anticipated start time or date or duration of the attack; and
- Counter-measures by the DoD or other federal agencies that might be attempted to thwart the attack.[180]

Here is how the White House describes what these Notices will contain and why all other information will be withheld:

179. Trope & Humes, *supra* note 152, at 3.

180. *See* Ozment, *supra* note 145 (demonstrating a lack of the considerations regarding imminent target notices).

> In information sharing there is always a risk: the risk of exposing our methods and intel sources, and we must balance that against the value of having the intel shared with industry. We have to weigh the risks with the benefits. But now, we are going to put our thumb on the scale, and we will press the scale to share more and respond less to the risk of revealing sources.
>
> When you get [the] information [contained in these Notices], you will see that *much of it is fragmentary and vague*. We may say your sector faces an unknown type of attack, at an unknown time, and of unknown intensity and we can't tell you more than that or how to use it. But you are [in] the best position to make use of that information.[181]

4. Cybersecurity Framework

While the EO's information-sharing directives aim chiefly at improving the "cyber hygiene" of critical infrastructure companies, the EO also aims to act where Congress did not and coax such companies towards adoption of a common set of cross-sector cybersecurity standards and best practices.[182] The EO directs the National Institute of Standards and Technology (NIST) to coordinate development of what the EO terms a Cybersecurity Framework (Framework), which it explains as a set of "voluntary consensus standards and industry best practices to the fullest extent possible."[183] The express purpose is to enable owners and operators of critical infrastructure to "identify, assess, and manage cyber risk."[184]

The EO directs NIST to complete the Framework by February 2014.[185] The latest development, as of this writing, is NIST's release, on October 22, 2013, of the Preliminary Cybersecurity Framework (Preliminary Framework).[186] Until a final draft appears, directors

181. *Id.* (emphasis added).

182. Exec. Order No. 13,636, 78 Fed. Reg. at 11,740–41.

183. *Id.* at 11,741.

184. *Id.*

185. *See id.* ("Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order . . . .").

186. *Improving Critical Infrastructure Cybersecurity: Preliminary Cybersecurity Framework*, NAT'L INST. STANDARDS & TECH., at i, http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf (last visited Dec. 27, 2013) [hereinafter

and management of critical infrastructure will be unable to assess what benefits or potential improvements, if any, the Framework will provide their company's cybersecurity.

The Preliminary Framework provides no examples of cross-sector standards or industry best practices, and thus its ultimate substance remains opaque.[187] Instead, the Preliminary Framework provides complex scaffolding for the Framework.[188] The Preliminary Framework explains that the Framework will be "composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers."[189] We focus here on the Framework Core, which the Preliminary Framework explains is "a set of cybersecurity activities and references that are common across critical infrastructure sectors . . . . The Core presents standards and best practices . . . for communication of cybersecurity risk across the organization . . . ."[190]

The Preliminary Framework provides a schematic of the Framework Core, instead of its substance. The Framework Core will consist of five "Functions": "Identify, Protect, Detect, Respond, [and] Recover."[191] The Preliminary Framework envisions the Framework Core as providing a "strategic view" for an organization's management of cybersecurity risk.[192]

The Framework purports to provide critical infrastructure companies with "guidance . . . on managing cybersecurity risk." The "guidance" consists first of encouraging organizations to "consider cybersecurity risk as a priority similar to financial, safety, and operational risk while factoring in larger systemic risks inherent to critical infrastructure."[193]

Preliminary Framework].

187. The Preliminary Framework emphasizes that it "relies on existing standards, guidance, and *best practices* to achieve outcomes that can assist organizations in managing their cybersecurity risk. By relying on those *practices* developed, managed, and updated by industry, the Framework will evolve with technological advances and business requirements." *Id.* at 1 (emphasis added). However, the Preliminary Framework gives no examples of cross-sector standards or best practices.

188. *See id.* at 2–3.

189. *Id.* at 2.

190. *Id.*

191. *Id.*

192. *Id.*

193. *Id.* at 1.

The Framework proposes a strategy that, on first reading, seems reasonable. The Framework disclaims any effort to "replace" an organization's existing cybersecurity risk management process and represents that it "complements" such process.[194] The Framework purports to offer organizations a method to "identify opportunities," which appears to be a euphemism for recognizing cybersecurity deficiencies. This becomes evident in the following passages from the Preliminary Framework:

> Profiles are . . . used to identify opportunities for improving cybersecurity by comparing a "Current" Profile with a "Target" Profile. The Profile can then be used to support prioritization and measurement of progress toward the Target Profile . . . . In this sense, Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.[195]

The Framework's authors, however, appear unaware or indifferent to the risks to which their methodology would expose an adopting organization. We see two sets of risks: one set related to the documenting of a company's "Current Profile" and "Target Profile," and one set related to the curious reference of communication "between organizations."

Regarding the risks from documenting Current and Target Profiles, the Framework proposes that an organization do a self-assessment of and describe its cybersecurity posture.[196] There is, however, no assurance that the resulting documented "current cybersecurity posture" would remain confidential and not be required to be disclosed, after a cyber intrusion or cyber attack, to regulators, government investigators, and potential plaintiffs. The Framework appears to proceed on the assumption that a company's "current cybersecurity posture" document would demonstrate that a company treated cybersecurity as a "priority." The Framework fails, however, to recognize that regulators, investigators, and plaintiffs in hindsight could cite such a document as evidence of the opposite, that the organization had a poor "current cybersecurity posture" and did not do as much as it should have to remedy and improve that "posture." Evidence of

194. *Id.* at 2.
195. *Id.* at 3.
196. *Id.* at 1.

that possible outcome appears in several passages in the Preliminary Framework, including:

> The Framework utilizes risk assessment to help organizations *select optimized target states* for cybersecurity activities.
>
> . . . .
>
> . . . A Framework Profile can be used to describe both the current state and the desired target state of specific cybersecurity activities, thus *revealing gaps that should be addressed* to meet cybersecurity risk management objectives.[197]

In the second quotation, the Preliminary Framework authors make the unwarranted and risky assumption that any cybersecurity "gaps" must be "addressed." It is for management and the board to decide which kinds of "gaps" should be addressed, and since cybersecurity is but one of several risks for which management and the board are responsible, it is not necessarily unreasonable or irresponsible for management and a board to decide that certain "gaps" will not be immediately addressed. However, the Framework's expressed position on this subject gives leverage to regulators, government investigators, and potential plaintiffs who can point to any unaddressed "gap" and allege negligence, malfeasance, or deficient cybersecurity. The first quotation contributes to that risk.[198] An improved "target state" is a relatively

197. *Id.* at 3, 7 (emphasis added).

198. One commentator on the Preliminary Framework has drawn similar inferences about the potential risks the Framework will create:

> The preliminary framework . . . what it will do if it takes hold is provide a common way for people to talk about and understand cybersecurity risks, and those people include regulators and judges, juries and others involved in deciding a lawsuit's outcome . . . .
>
> . . . .
>
> The reality is that as private parties are litigating issues related to companies' security practices and compliance with industry standards, it is highly foreseeable that litigants will refer to the framework as a statement of industry standards . . . .
>
> Even if a company is following the practices set forth in the framework, it can still run the risk of being faulted by private parties for describing its practices in a way that is inconsistent with the common language established by the framework . . . .

Allison Grande, *Cybersecurity Framework Risks Becoming Litigation Fodder*, LAW360 (Oct. 25, 2013, 9:24 PM), http://www.law360.com/privacy/articles/483418?nl_pk

neutral position, but advocating that organizations "select optimized target states" imposes a responsibility on adopters of the Framework to make sure that the "target state" they select is appropriately high enough to be "optimal." If they fail to do that, they may be at considerable risk.

Similarly, the Framework proposes that an organization "describe" its "target state for cyber security," but here again there is no assurance that the resulting documented "target state" would remain confidential and not be subject to enforceable demands that it be disclosed to regulators, government investigators, and potential plaintiffs. Each such recipient could second-guess an organization's selection of its "target state" and criticize the pace of progress from "current posture" to "target state." It is not clear that the "business judgment" rule would protect a board from such second-guesses. Unless there is some assurance of immunity (which would require a congressional enactment), companies that document their Current and Target Profiles might be able to point to them as evidence of treating cybersecurity as a priority and acting responsibly, but in a post-cyber-attack context where judgments can be easily swayed and skewed by hindsight, a company could be exposing itself to risks when the purpose of the exercise should be limited to improving a company's resilience to cyber attacks.

The second set of risks, related to communications "between organizations," finds evidence in both the Preliminary Framework and in the press release that accompanied it. The Framework will purportedly provide a "common language to communicate requirements among interdependent partners responsible for the delivery of essential critical infrastructure services. Examples include: . . . A critical infrastructure sector may establish a baseline Target Profile that can be used among its constituents as an initial baseline."[199]

If a sector establishes a Target Profile for its "constituents," then the Framework's authors are encouraging the use of the Framework as an involuntary and enforceable device, which is contrary to what the EO represented it to be. Our impression—that

=367d7227-22e4-438f-90bd-9b35 (quoting Ronald Lee, a partner at Arnold and Porter LLP, and Gerald Ferguson, a privacy, security, and social media team co-leader at BakerHostetler).

199. *Preliminary Framework*, *supra* note 186, at 12.

the Framework's authors intend the Framework to serve as an enforcement of cybersecurity standards—is further supported by a statement in NIST's press release that accompanied release of the Preliminary Framework: "The framework will foster communications among internal and external stakeholders and help organizations *hold each other accountable* for strong cyber protections . . . ."[200]

We think such statements portend an unfortunate evolution in the Framework, from a purportedly "voluntary" mechanism into an involuntary enforcement device that a "sector" or another organization might use to hold an adopting organization "accountable" for a lack of cyber protections. Thus, although announced as a means for reducing cyber risks, we think that the Framework as currently drafted and as described by its authors is evolving into a mechanism that will increase, rather than decrease, a company's risks.

In light of the risks the Framework might create, it is all the more important that the document be clear and easily understood by board and C-suite officers. Unfortunately, the Preliminary Framework is a formidable and unwieldy read for directors and officers, because of the additional schema that is attached to it in the form of an identification of "underlying key Categories and Subcategories for each of these [five] Functions, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory."[201]

One of its infirmities is that the Preliminary Framework tries to do too much for too many segments of critical infrastructure interests: "The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program."[202]

The following example provided by the Preliminary Framework illustrates the complexity and the cross-referencing that readers will have to navigate and sort through to comprehend:

200. Press Release, NIST, NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments (Oct. 22, 2013), http://www.nist.gov/itl/cybersecurity-102213.cfm (emphasis added).

201. *Preliminary Framework*, *supra* note 186, at 2.

202. *Id.* at 11.

> For instance, the "Protect" Function, categories include: Data Security; Access Control; Awareness and Training; and Protective Technology. [At the next level down,] *ISO/IEC 27001 Control A.10.8.3* is an informative reference which supports the "Data during transportation /transmission is protected [sic] to achieve confidentiality, integrity, and availability goals" Subcategory of the "Data Security" Category in the "Protect" Function.[203]

We think that any director or officer will need fortitude, patience, and more time than they can spare to comprehend that passage. We doubt that counsel will find it easy to explain to a board because the illustrative passage is so ungrammatical and complex that a framework consisting of such passages will turn a proposed cybersecurity tool into a blunt, useless instrument.

What we think boards and management of BPS companies will probably be most interested to know is whether the Framework, when published in final form, will create another set of standards and recommendations that compete with those already published and in preparation by NERC and its Task Forces (or any other critical infrastructure regulator). Boards and management will also want to know whether the Framework shares a common objective or places priorities on the same cybersecurity efforts as those expressed in the NERC Task Force reports.

On the question of whether the Framework will be intended or might become a set of standards that compete with other standards applicable to BPS companies, there are two answers—one clear, the other speculative. The clear answer is that the Framework is derived from an executive order, not from a federal statute or regulation issued pursuant to a federal statute. Therefore, unless later incorporated into a statute or adopted by NERC as part of a CIP Standard (which is highly improbable), it cannot be binding on BPS companies. The EO cannot require a critical infrastructure company to adopt and implement the Framework's standards and best practices (that will appear in its Framework Core[204]).

203. *Id.* at 2.

204. The Framework Core is described in the Preliminary Framework as a set of cybersecurity activities and references that are common across critical infrastructure sectors and organized around particular outcomes. *See id.* at 2. The Framework Core presents standards and best practices in a manner that allows for communication of cybersecurity risk across the organization from the senior executive level to the implementation/operations level. *See id.* at 2.

Moreover, once released, the Framework will be available for companies to consider. If companies decide to adopt it, there would appear to be no authority in the EO to require an adopting company to accept the entire Framework or to adhere to it after adoption. However, there are unconfirmed reports that when Catastrophic Target Notices are issued to the approximately one hundred companies that appear likely to be so identified, these Notices will include a statement "encouraging" the recipient to adopt the Framework. Expressed in that context, such an invitation may be perceived as an invitation a company should be careful not to refuse, which is therefore a coercive use of the Notices and further evidence that the Framework is evolving away from a "voluntary" set of standards.

In addition, presumably, companies may pick and choose among the standards and best practices that they think most suitable for their operations and security risks—and that fit the budget they are willing to allocate to the effort. As companies improve their enterprise-wide cybersecurity profile, they may find that certain Framework standards cease to be applicable or relevant and may decide that other standards in the Framework are useful. The Preliminary Framework does not address such issues or whether there would be a coherent result if companies could, from time to time, decide what parts of the Framework they will use and what parts they will no longer use. The Preliminary Framework does, however, offer users the option to adopt and use some of the scaffolding offered in the Basic Overview.[205] It also, as noted above, emphasizes the need to address any "gaps" found between Current and Target Profiles, which makes the Framework appear something other than "voluntary."

The speculative answer derives from another way in which the Framework's standards could achieve a nearly binding status. Consider the result of the following events occurring: first, the President and other executive branch officials make repeated

205. The Preliminary Framework states that organizations can choose the details and their capabilities already implemented in the five "high-level Functions" identified in the Framework Core: identify, protect, detect, respond, and recover, emphasizing that critical infrastructure companies should have at least basic capabilities implemented in each of these areas and can begin to review what particular categories and subcategories they currently use to help achieve those outcomes. *Id.* at 11.

public statements about the national security need for companies to adopt the Framework in order for critical infrastructure to be protected from cyber attacks; second, the President and other executive branch officials then ask companies to disclose if they have formally adopted the Framework; and third, thereafter the DHS posts on one of its websites a list of the early adopters of the Framework (and DHS updates that list as others adopt the Framework). In that event, critical infrastructure companies that have refrained from or decided against adopting the Framework or disclosing their status would in all likelihood experience considerable public pressure. If, despite such pressure, they did not then adopt the Framework (while others in their sector had adopted it) or opted against disclosing their status, they almost certainly would experience substantial reputational damage among other adverse consequences.

Benchmarking may also force such companies to respond in a manner similar to their peers. Their boards and management might decide that, similar to the receipt of Catastrophic and Imminent Target Notices, a failure to adopt the Framework might impart enhanced corporate cyber responsibilities to ensure that notwithstanding that failure, the company has taken all reasonable actions to improve its cybersecurity. Companies may decide that there are greater risks in being identified—publicly or in a post-cyber-attack lawsuit or regulatory enforcement action—as an adopter of the Framework (i.e., arguing that "adoption shows we took reasonable precautions") than as an abstainer (i.e., arguing that "we thought we knew ways to improve our cybersecurity better than those in the federally developed Framework"). In short, boards and management will need to be aware that non-adopting companies may experience a variety of forms of "shunning" and "shaming" and that third parties—including customers, suppliers, insurers, and other stakeholders—may condition terms of agreement on a demonstration that the company adopted and implemented the Framework. It is not hard to imagine, for example, that a major customer could demand that all of its suppliers certify that they have adopted and implemented the Framework.

This conclusion is reinforced by language in the EO that suggests the Framework may not even be intended as "voluntary" but is to be treated as something companies can be coaxed or pressured into adopting. Consider the following passage from the

EO: "The Cybersecurity Framework shall include guidance for *measuring the performance* of an entity in implementing the Cybersecurity Framework."[206]

If the Framework is intended to be "voluntary" and allows companies (as the Preliminary Framework explains) to "leverage the Framework . . . to improve an organization's management of cybersecurity risk,"[207] then there should be no need for a means of "measuring the performance" of companies as they adopt or selectively implement the Framework. The EO's language of "measuring the performance" suggests that the White House might already be considering ways to apply public pressure to companies that ignore or that elect not to adopt the Framework. Once they do adopt it, they may be subject to federal government publication of whether the measurement of their performance in "implementing" the Framework meets White House or DHS approval or disapproval.

There is, however, an alternative interpretation to the metric language in the Framework.[208] It will be offered to companies for self-assessments of their progress in implementing the Framework. We notice that the Preliminary Framework contains, in

206. Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,741 (Feb. 19, 2013) (emphasis added).

207. *Preliminary Framework*, *supra* note 186, at 2.

208. The Preliminary Framework points to the use of current and target profiles as a resource for users to prioritize and measure progress toward the target profile while considering other sector-specific factors and business needs including cost-effectiveness and innovation. Therefore, profiles can be used to conduct self-assessments and communicate within an organization or between organizations. *Id.* at 3. Compare the Preliminary Framework to the NERC CATF Report, which includes NERC's own framework, developed by a working group of the Critical Infrastructure Protection Committee, featuring what NERC calls "attack trees." *See* CATF REPORT, *supra* note 13, at 4. These attack trees provide a solid structure to build on, such as for each revision to the CIP Standards, allowing new requirements to be incorporated into the attack trees and analysis rerun to determine any positive or negative consequences of the proposed changes. NERC recommends to compliance entities that, prior to release of a NERC Alert, the BPS operator should compare mitigation measure actions against the attack trees to determine if the recommendations provide the greatest likelihood of reducing the potential for compromise. At least annually BPS operators should evaluate the attack trees to incorporate new information. CATF REPORT, *supra* note 13, at 33. Clearly, the Preliminary Framework offers a meaningless structure compared to the industry-specific framework presented by NERC, so critical infrastructure companies in the energy sector will find little value in the Preliminary Framework.

Appendix C, Section C.3, a discussion entitled "Conformity Assessment," which purports to provide guidance for a company's self-assessment of its implementation of the Framework:

> Industry has a long history of developing conformity assessment programs to meet society's needs.
>
> An organization can use conformity assessment activities to assess the implementation of requirements related to managing cybersecurity risk. The output of conformity assessment activities can enhance an organization's understanding of its implementation of a Framework profile.[209]

That language discusses a company's *self-assessment*. By contrast, the EO's language appears to request a way for "measuring the performance of an entity"[210] by outsiders, and probably DHS. Moreover, a later passage in the same section suggests that NIST contemplates these self-assessments to be *made public*,[211] which would expose a company to considerable risks when customers, suppliers, lenders, and insurers view and evaluate the company's self-assessment of its implementation of the Framework. The Preliminary Framework emphasizes the public disclosure of such assessments, the need for "confidence" in them by third parties, and the disadvantages that might flow from failing to conform with the Framework and having others in the market *know* it:

> The need for confidence in conformity assessment activities must be balanced with cost to the private and public sector including, . . . additional legal obligations, and the cost of non-conformity in the market. Successful conformity assessment provides the needed level of confidence . . . . Critical infrastructure's evolving implementation of Framework profiles should drive the identification of private sector conformity assessment activities that address the confidence and information needs of stakeholders.[212]

That passage appears to assume that "conformity [to the Framework] assessments" should (and will) be made public, that transactors will rely on them in negotiations of deals, and that such

209. *Preliminary Framework*, *supra* note 186, at 37.
210. 78 Fed. Reg. at 11,741.
211. *Id.*
212. *Preliminary Framework*, *supra* note 186, at 37.

assessments are essential to provide "the needed level of confidence."[213]

We doubt that boards and management will welcome being publicly pressured into adopting the Framework, but that appears to be the intent of the EO and the Preliminary Framework. We also doubt that boards and management will approve public release of a company's own "conformity [to the Framework] assessment" or one conducted by a third party. Critical infrastructure companies no doubt find it important to know if their suppliers, customers, lenders, and insurers are reliable and may view cybersecurity as among the crucial indicia to be considered during negotiations of a transaction. But such negotiations and the accompanying "due diligence" are an appropriate and risk-based way for parties to examine each other's reliability to perform the terms of an agreement. The parties can then modify those terms to reflect the findings of their respective "due diligence" reviews. Although NIST may be eager to have the Framework exert a strong influence on the commercial and financial markets, if that proves to be the case in the final draft and interpretation of the Framework by the executive branch, then we think that will dissuade many companies from adopting the Framework.

We should add that comments by White House officials give the clear impression that DHS will be directed to use the Framework to "bootstrap" and enhance existing cybersecurity regulations, creating yet another way by which the Framework's standards will not really be "voluntary." As the White House Senior Director for Cybersecurity explained shortly after issuance of the EO:

> So once we have this Cybersecurity Framework in a year—what will we do? In regulated industries, we will ask the regulators to look at the Framework, but we are not seeking change for change sake, and if the industry is in good shape, we won't ask them to change. But some regulators need to improve, and we will ask them to consider the Framework and to issue new regulations through the usual process of issue, ask for comment, revise and reissue . . . . If you have read the Executive Order, there is not a lot of description of this voluntary program—because we want industry to help us identify

213. *Id.*

> what would be a helpful program and encourage participation in it.[214]

Finally, if boards and management ask whether the Framework's "core" of standards and best practices share common objectives and priorities with those expressed in NERC's CATF and SIRTF Reports, the answer at this point appears to be that the Framework aims at a much lower set of objectives—daily cyber hygiene of companies—not at helping them prepare for the worst of all possible post-attack scenarios flowing from Severe Events. Recall that the White House Senior Director for Cybersecurity emphasized that "cyber hygiene will not protect you" from the adversaries' A-Game—Advanced Persistent Threats—but that is not the Framework's objective.[215] Instead, it is to be designed to "help companies that are the least sophisticated to bring them up the curve in cybersecurity" and thus improve the cyber hygiene of critical infrastructure throughout the nation, thereby forcing the adversaries to use their "A-Game."[216]

We think that whatever standards and best practices NIST does eventually place within that schematic, none appear likely to address the Severe Event and New Normal challenges identified by the SIRTF Report.[217] Our view is not changed by the fact that the Preliminary Framework contains the following description of the fifth "Core" element:

> *Recover*—Develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the capabilities or critical infrastructure services that were impaired through a cybersecurity event.[218]

Rather than reflecting a convergence of the EO's objectives and NERC's Task Force objectives, that passage suggests a serious gap. The post-attack consequences envisioned by that passage are not as disruptive, damaging, and enduring to BPS operations as a Severe Event, as evidenced by the characterization of the recovery or restoration effort as seemingly simple, straight-forward, and requiring no new preparations, just an application of the usual

214. Ozment, *supra* note 145.
215. *Id.*
216. *Id.*
217. *See* SIRTF REPORT, *supra* note 13.
218. *Preliminary Framework*, *supra* note 186, at 7.

methods. That is quite unlike the Task Force view that the electricity industry lacks experience in "planning for and responding to high-impact events that have a low probability of occurring or have not yet occurred."[219] For that reason, the SIRTF Report focused its recommendations on a Severe Event that "stresses the electricity industry's capabilities well beyond its already robust emergency response capabilities"[220] and thus beyond any company's "comfort zone" of existing plans and table-top exercises and other rehearsals.[221] In short, these are situations for which there is no prior experience to draw upon—and the planning therefore needs to be imaginative and resourceful. Thus the SIRTF Report gives concrete examples of kinds of post-attack circumstances that will go beyond a BPS company's prior experience and should be anticipated:

> - The event is beyond the scenarios typically exercised by entities as part of the NERC Emergency Preparedness and Operations standards.
>
> . . . .
>
> - As a result of insufficient generation and transmission resources, system operators must shed load without advanced notice and regularly implement rotating blackouts to manage BPS reliability.
>
> . . . .
>
> - Multiple information technology and communications have failed-entities contend with issues that restrict the ability of system operators to effectively communicate, operate, and monitor the BPS.
> - The event is persistent or recurring throughout the mitigation and restoration phases, further hindering recovery and restoration.
>
> . . . .
>
> - BPS entity staff experience a high degree of physical and psychological demands for an extended period of time.
>
> . . . .

219. CATF REPORT, *supra* note 13, at 1.
220. SIRTF REPORT, *supra* note 13, at 10.
221. *Id.*

- The resources required to respond exceed the financial capacity of some entities.[222]

The Preliminary Framework makes no effort to prepare critical infrastructure for such realities.[223] As a result, there is a significant and perplexing gap between the Preliminary Framework and the NERC Task Force reports in what each contemplates as consequences from the cyber-attack threats, in the kind of attacks (kinetic or non-kinetic, operational target or business information target) they are most concerned to address, in their respective objectives, and in the preparations that each recommends. The more one compares the recommendations to be expressed in the Preliminary Framework and the recommendations contained in the NERC Task Force reports, the wider the gap appears to be between their objectives and the actions each seeks to persuade BPS owners and operators to pursue to improve cybersecurity. As a result, this gap is so wide it may force companies to choose which set of objectives—and which set of plans and preparations—to pursue. This is because companies have limited resources and the need to train personnel to implement one set of recommendations may make it impossible for many critical infrastructure companies to respond to both to the Preliminary Framework (as intended by the White House) and to the NERC Task Force recommendations (as intended by NERC and its trustees who approved the Task Force reports).[224] Moreover, the need to make such a choice may become more compelling because the gap between these objectives will widen as the adversaries continue to improve their capabilities to launch cyber attacks that target, damage, and disrupt critical infrastructure. The gap between those two objectives—cyber-hygiene improvements and Severe Event preparations—should give boards and management some cause for concern and make them

222. SIRTF REPORT, *supra* note 13, at 11 (footnote omitted).

223. The Preliminary Framework's introduction describes the document as providing guidance to an organization on managing cybersecurity risk. It states that its key objective is to "encourage organizations to consider cybersecurity risk as a priority similar to financial, safety, and operational risk while factoring in larger systemic risks inherent to critical infrastructure." *Preliminary Framework*, *supra* note 186, at 1.

224. SIRTF REPORT, *supra* note 13, at 1; *see also* CATF REPORT, *supra* note 13, at 1–2, 12–13.

wonder which should be the higher priority for their company in the immediate future.

We worry that adoption and implementation of the Framework will increasingly be viewed in illusory and misleading terms, for example, as meeting a high standard (which it is not) and as fulfilling the White House summons to private industry to help protect national security (which it surely will not do since it does not address Severe Events and their catastrophic consequences). It is ironic that the same EO that directs that DHS identify critical infrastructure that could cause widespread damage regionally or nationally if damaged by cyber attacks, nonetheless aims with its Framework at the lowest of objectives—a removal of easy targets from the adversaries' reach.

Moreover, we think that the White House's rationales for the Framework will prompt some boards and management to ask their counsel, *"If the Framework is designed to force sophisticated, well-funded and presumably state-sponsored adversaries to shift to and invest heavily in their 'A-Game,' shouldn't we be preparing for that? The Government isn't saying it will protect our company from advanced persistent threats, so isn't the strategy going to put our company at greater risk of successful and damaging attacks?"* The Preliminary Framework appears to overlook those questions, but those and similar questions will almost certainly be at the core of discussions by boards and management of what response their company should be making to the implementation of the EO; to the receipt of Catastrophic Target Notices and Imminent Target Notices; and to the "encouragement" to adopt the Framework followed by "conformity assessments" (whatever they turn out to be). Addressing the probable results of a successful coordinated cyber attack that seeks to cause kinetic damage to BPS operations remains the focus of NERC's CATF and SIRTF Reports. As a result, these reports take a much longer and more critical view of what characteristics in a kinetic cyber attack could destabilize and damage BPS company operations.[225]

We also note that the Preliminary Framework may create the unintended consequences that have resulted from other sets of standards; namely, the encouragement of a "compliance culture"

225. In the next section, we will briefly review some of the recommendations contained in those reports, but only to identify some that highlight why boards and management of BPS companies may want to focus more on these recommendations than on the Preliminary Framework.

that focuses solely on meeting the applicable standards' requirements and encouraging companies to believe that will be sufficient. The General Accountability Office (GAO) warned of such results from cybersecurity standards back in January 2011 (two years before the EO):

> *Utilities are focusing on regulatory compliance instead of comprehensive security.* The existing federal and state regulatory environment creates a culture within the utility industry of focusing on compliance with cybersecurity requirements, instead of a culture focused on achieving comprehensive and effective cybersecurity. Specifically, experts told us that utilities focus on achieving minimum regulatory requirements rather than designing a comprehensive approach to system security. In addition, one expert stated that security requirements are inherently incomplete, and having a culture that views the security problem as being solved once those requirements are met will leave an organization vulnerable to cyber attack. Consequently, without a comprehensive approach to security, utilities leave themselves open to unnecessary risk.[226]

Moreover, there is considerable controversy concerning the prolonged, staggered approval and adoption of various overlapping versions of CIP Standards by NERC and the significant deficiencies in those currently applicable. Such delays and deficiencies result in the BPS companies continuing to be seriously deficient in their cybersecurity defenses and preparations for addressing the consequences of a Severe Event and New Normal of degraded operations and services. The extent to which cybersecurity deficiencies continue to exist in this sector were reported in a Department of Energy Inspector General Audit Report, issued in January 2011:

> Despite their importance to protecting the power grid, the CIP standards did not include a number of security controls commonly recommended for government and industry systems. . . . In certain cases, Commission officials noted that the lack of stringent requirements for defining

226. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-117, ELECTRICITY GRID MODERNIZATION: PROGRESS BEING MADE ON CYBERSECURITY GUIDELINES, BUT KEY CHALLENGES REMAIN TO BE ADDRESSED 23–24 (2011), *available at* http://www.gao.gov/new.items/d11117.pdf.

> critical assets contributed to significant under reporting of these assets.[227]

For example, the CIP Standards did not clearly define what constituted a critical asset or critical cyber asset. Absent a standard definition, entities that are part of the bulk electric system were permitted to use their discretion when identifying critical assets and critical cyber assets, a practice that could have allowed them to determine whether the cybersecurity standards were even applicable to their organization. Specifically, if an entity determined that no critical assets or critical cyber assets existed, it was exempt from the remaining original CIP Standards.[228]

VI. CYBERSECURITY RECOMMENDATIONS BY NERC'S CATF REPORT AND SIRTF REPORT

Unlike the Framework, which attempts to collect a core of cross-sector standards and best practices, the CATF and SIRTF Reports offer recommendations and guidance as points of departure from which companies may then develop plans and preparations that will fit the kinds of damage such operations might experience during and after the first wave of a coordinated cyber attack.[229] As explained by the SIRTF Report:

> The suggestions offered throughout this report are intended to prompt entities to develop their own approaches and flexible plans that would be applicable under a wide variety of circumstances. . . . Entities are encouraged to critically examine their current capabilities, and to consider what else they may need to do to manage restoration and operations during a Severe Event.[230]

227. OFFICE OF AUDITS & INSPECTIONS, U.S. DEP'T OF ENERGY, AUDIT REPORT: FEDERAL ENERGY REGULATORY COMMISSION'S MONITORING OF POWER GRID CYBER SECURITY 2 (2011), *available at* http://energy.gov/sites/prod/files/igprod/documents/IG-0846.pdf.

228. *Id.* The Inspector General noted that FERC, in exercising its responsibility to oversee and approve NERC's cybersecurity standards, "had not always acted to ensure that the cybersecurity standards" NERC proposed "were adequate. In addition, [FERC] had not always effectively monitored how NERC and the regional entities assessed implementation of the cybersecurity standards." *Id.*

229. SIRTF REPORT, *supra* note 13, at 7.

230. *Id.*

The SIRTF Report inferred that, having mapped out Severe Event scenarios and described what a New Normal post-attack period of reduced reliability of services might be like, NERC would be asked by BPS boards and management whether, during a Severe Event and post-attack New Normal period, entities could be exempt from compliance with the FERC-approved CIP Standards for cybersecurity developed and proposed by NERC.[231] The SIRTF Report observes that the standards should still apply, but realistically noted that violations in these circumstances would probably occur:

> The SIRTF reviewed the NERC standards and concluded that standards support safe and reliable operation and should be applicable during a Severe Event. While it is conceivable that during a Severe Event an entity will violate certain standard requirements given the intensity of planning and operating challenges through the New Normal period, it would be impossible to predict these circumstances in advance.
>
> . . . . Although a Severe Event may put entities in a position where they cannot comply with all [CIP cybersecurity] standards, entities are in the best position to "do the right thing" for reliability and public safety, and self-report any violation of NERC standards as time and circumstances permit.[232]

Although the SIRTF Report decided against recommending suspension of the applicable CIP Standards during and after a Severe Event, it suggests that if violations in those challenging circumstances occur, the penalties imposed might be substantially reduced provided that the entity acted to reinforce and restore reliable operations and self-reported all violations when the crisis had subsided sufficiently.[233] Note, however, that the New Normal is not merely a period of reduced services. In the context of BPS operations, NERC, in the CATF and SIRTF Reports, consistently emphasizes that what most characterizes the New Normal is that the "BPS is operated at a reduced state of *reliability and supply* for months or possibly years."[234]

231. *Id.* at 17.
232. *Id.* at 7–8.
233. *Id.*
234. *Id.* at 2 (emphasis added).

A review of the recommendations by the CATF Report and SIRTF Report reveals that, while most recommendations concern internal operations unique to a BPS entity, several would be important for owners and operators of other critical infrastructure to be aware of and take into account when attempting to understand what impact a Severe Event and New Normal of reduced reliability and supply of electric power would have on their operations. Knowing those impacts should enable such entities to make preparations accordingly, and thus be spared the chaos and confusion that might otherwise result from being confronted with unanticipated and unimagined challenges.

We therefore limit our discussion to the recommendations in the CATF and SIRTF Reports that have a wide cross-sector application. As a result, we omit discussion of important Severe Event and BPS operational issues, such as "real-time assessments" and "step-by-step restoration procedures," and instead concentrate on the formation and stabilization of "islands" of electric power through "load shedding" (rotating outages) and the jury-rigging of "situational awareness" needed for stabilizing the "islands" and the recovery efforts. These activities need to be understood by other critical infrastructure, and the CATF and SIRTF Reports therefore deserve to be read by management and discussed by boards of such companies. When doing so, it would help to remember that, unlike NERC-developed, FERC-approved CIP Standards, or the NIST-prepared Preliminary Framework with its "core" of standards and best practices, the recommendations in the CATF and SIRTF Reports are *not standards nor intended to set a minimum level of assurance for a check-box compliance-driven company*. The reports' recommendations are instead designed to *prompt companies to consider what they might do to improve their management of the consequences following a Severe Event cyber attack*.[235] Thus, the emphasis is on helping a company carefully think through its manageable, best courses of action when challenged by the probable, worst-case scenario of a Severe Event.

Thus, unlike the White House strategy of emphases on cyber hygiene and defense through voluntary adoption of cybersecurity standards, NERC's CATF and SIRTF Reports assume the worst—that adversaries can and someday may cause a Severe Event by

235. *See id.* at 9–10.

cyber attacks that target the BPS.[236] The NERC reports therefore assume that, instead of the futility of defending what is, and will likely remain, vulnerable to attack, BPS companies should put their emphasis on managing "restoration and operations during a Severe Event." The SIRTF Report explains:

> This report examines the aspects of emergency operation and restoration that would be particularly challenged through a Severe Event and provides options to enhance the resilience[237] of the bulk power system. The suggestions offered throughout this report are intended to prompt entities to develop their own approaches and flexible plans that would be applicable under a wide variety of circumstances. . . . Entities are encouraged to critically examine their current capabilities, and to consider what else they may need to do to manage restoration and operations during a Severe Event.[238]

With those objectives and emphases in mind, we now look at what may be the most unfamiliar aspect (and most important for other critical infrastructures to learn): how the BPS might attempt to recover from a "severe event."

A. Formation of "Electrical Islands" Following Severe Events

Each company managing a critical infrastructure operation depends on the reliable supply of electric power for its survival. For such companies to be prepared for the worst-case scenario, such as that of a cyber-attack Severe Event, they should give consideration to reviewing the preparations for Severe Events and the post-attack New Normal being made by the operators of the BPS services on which they rely. The better that an electric power customer knows and understands how the BPS operator will handle that crisis, the better the chances the critical infrastructure customer has of enhancing its own plans to be in a position to maximize cooperation with the BPS operator and to have contingency plans that address the potentially catastrophic consequences.

236. CATF REPORT, *supra* note 13, at 2; *see* SIRTF REPORT, *supra* note 13, at 19–20.

237. As used in the SIRTF Report, "resilience" is "generally defined as the ability to recover or adjust to misfortune or change." SIRTF REPORT, *supra* note 13, at 11.

238. *Id.* at 7.

Perhaps foremost among the preparations recommended by NERC's SIRTF Report are those for managing "graceful degradation"[239] (a concept that may be quite unfamiliar to operators and owners of other critical infrastructure), as well as stabilizing, repairing, and expanding "electrical islands."[240] If a critical infrastructure company relies on the BPS and has not considered how it would cope during the New Normal period being located inside a surviving "electrical island" (with rolling outages)—or worse, outside such "islands"—then such a company's cybersecurity plans will leave it unprepared for the worst circumstances and at high risk of being overwhelmed when it might otherwise have coped with them. Let's consider how the "islands" would form and some of the SIRTF Report recommendations of preparations for stabilizing them.

1. Characteristics of Post-Severe Event "Islands"

The SIRTF Report assumes that immediately following (or during) a persistent Severe Event, "islands are likely to form as transmission lines between areas of the system trip."[241] These islands would be far smaller than the four major "Interconnections."[242] The SIRTF Report assumes that "a substantial number of supply resources are unavailable for an extended period of time and as much as or more than 50% of total instantaneous demand cannot

239. In the event of a severe cyber attack on the BPS, NERC's CATF Report observes that survivability involves focusing on protecting those systems and functions that are essential to maintaining reliable operations. Reliable operations will degrade over time, resulting in the gradual reduction in services and functions until essential operations are no longer possible. "The key is trying to maintain reliable operations in a reduced state for as long as possible. This resilience characteristic is known as graceful degradation of service." CATF REPORT, *supra* note 13, at 28.

240. Upon a Severe Event, "[r]ather than operating as part of a large interconnected (and therefore more stable) grid, system operators may need to manage a number of small 'electrical islands' and implement load shedding or rotating blackouts for extended periods of time (weeks, months, or years)" until the interconnected grid stabilizes and returns to pre-incident normal. These islanding scenarios might have to be the New Normal for a BPS operator. SIRTF REPORT, *supra* note 13, at 3.

241. *Id.* at 20.

242. *See id.* at 18.

be served in the islands."[243] These "islands" would be unstable.[244] They might have to be operated by entities that "are not normally responsible for system operator functions."[245] The substitute operators would be further challenged by the duration of instability and their lack of experience in prolonged stabilizing activities such as "load shedding"[246]:

> [E]xperience with implementing load shedding plans has been limited to relatively short periods of time—a few hours or at most a day or two. In contrast, under Severe Event conditions, rotating blackouts may need to be implemented for an extended period of time and for significantly longer rotation intervals.[247]

While "[l]arge interconnected power grids are inherently stable because they have many sources of governor-controlled generation and relatively predictable load patterns,"[248] the smaller "islands" formed following a Severe Event would provide electrical power of uncertain reliability: "Islands with small amounts of generation and load have less inertia and as such experience larger frequency swings, are harder to control, and are more likely to collapse from subsequent generation loss than are the existing four Interconnections."[249]

Thus, being within an "island" of electric power would improve a company's chances of being able to continue operations (albeit at a degraded level between scheduled rolling outages) or to restore full operations at the earliest practicable time. However, being within an "island" would provide no certainty of being able to receive electric power. Moreover, the instability of the "island" would pose risks to critical infrastructure, computers, and other equipment that can be damaged by surges and drops in frequency or voltage. These are risks that would need to be addressed in such companies' Severe Event planning and preparations:

> [M]any of today's loads are frequency or voltage sensitive or both (such as computers, industrial control systems,

243. *Id.* at 19.
244. *See id.* at 18.
245. *Id.*
246. *Id.* at 25.
247. *Id.* at 18.
248. *Id.* at 23.
249. *Id.* at 20.

> [and] other electronic devices) and may trip off-line as a result of these swings. The challenge with frequency or voltage sensitive load loss [for electric power customers and their sensitive equipment] is that it will come back on the system once electrical parameters are within the prescribed range. Also this can be further complicated with the increase in automatic schemes within the distribution system for "self healing" (smart grids). This uncoordinated load restoration possibly increases the risk of island collapse.[250]

2. Use of "Load Shedding" to Build and Stabilize "Islands" and Need for Information Sharing

In the immediate aftermath of a Severe Event, BPS operators will probably find that, in order to manage the load-generation balance, they must resort to "load shedding."[251] A BPS operator in control of an "island" cannot supply all customers equally and will need to set priorities among its customers. Knowing that these decisions need to be made should alert owners and operators of other critical infrastructure of the need to discuss the issue in advance with not only their regular BPS operator but any others who might become responsible for control of an "island" containing these other critical infrastructure companies. The discussions will need to cover being excluded from "load shedding" areas and developing strategies for maintaining communications so that critical infrastructure companies will know the amount of power that will be available to them and when power may be lost. As the SIRTF Report explains:

> Load shedding plans need to consider the priority or importance of loads such as critical power system loads and other dependent critical infrastructures such as telecommunications.
>
> . . . .
>
> . . . [It is important to e]nsure that critical power system loads and other critical infrastructure loads such as certain telecommunications centers are excluded from load shedding plans.
>
> . . . .

250. *Id.*

251. *See id.* at 25–27 (load shedding).

> In the event of sustained rotational load shedding (rotating blackouts) communication becomes a key factor to ensure that affected areas understand what power supply they will have, at what time[,] and for how long. . . . [T]hese communications need to be carefully considered and coordinated with local distribution companies, local law enforcement agencies, emergency responders[,] and government officials.[252]

More companies than just telecommunication critical infrastructure companies need to be involved in such planning and discussions. For example, the experience with Hurricane Sandy and the rapid depletion of gasoline at service stations[253] suggests that, although service stations are often not viewed as high-priority customers during an emergency recovery, they need to be considered for that priority in preparations for a Severe Event. However, the SIRTF Report cautioned that, as with the other recommendations, these are not standards for rigid adoption, but guidance from which companies can then develop their own plans and preparations which, by necessity, must be flexible and should seek to be more comprehensive and more customized to their circumstances and operations than CIP and other cybersecurity standards. Instead, companies need to coordinate their plans and negotiate information sharing agreements so that when the extent of the damage and outages becomes known they can work together to develop plans for the New Normal of "electric power islands." As the SIRTF Report explains:

> Since it is impossible to predict the extent of islanding formation following a Severe Event, it may not be practical to share operational information ahead of time. It is important therefore that information-sharing stra-

252. *Id.* at 25–26.

253. New Jersey's largest electric utility, Public Service Electric & Gas Company, has explained to its state regulatory body, the New Jersey Board of Public Utilities, that during the immediate aftermath of Hurricane Sandy, many gasoline service stations were without power at a time when many residents needed gasoline to fuel emergency generators. Access to gasoline, therefore, became a much more severe crisis than simply a matter of mobility, and it became necessary to expedite storm restoration efforts to prioritize service stations. *Cf. In re Petition of Public Service Electric and Gas Company*, PUB. SERV. ELECTRIC & GAS CO. ¶ 85 (Feb. 20, 2013), http://www.pseg.com/family/pseandg/tariffs/reg_filings/pdf/EnergyStrong.pdf.

> tegies are established in preparation for such events to expedite this information dissemination and address any confidentiality concerns.[254]

In reviewing information-sharing agreements, BPS operators and other critical infrastructure companies will also need to review the probable impairment of communications following a Severe Event and how they will communicate during the New Normal period in order to share information and maintain situation awareness despite misinformation that might be generated by the cyber attack's malware.

3. Severe Event Impact on Communications Infrastructure

Because of the moment-to-moment need to balance loads and other delicate potential triggers of cascading outages, the BPS is heavily dependent on communications infrastructure, and Severe Events to the BPS cannot be realistically discussed without discussing the impaired communications that would result and their impact on detecting a cyber attack, as well as managing efforts at stabilizing "electric islands" after a Severe Event. Other critical infrastructure needs to be aware that the widely dispersed operations of the BPS make the reliable flow of accurate (not cyber-corrupted) communications vital to BPS reliability. As the SIRTF Report explains:

> The reliable operation of the BPS depends on a highly reliable communications infrastructure. North America's BPS has been described as the world's largest machine; generation resources, consumer load, field operations, and centralized controls are all separated by significant geographic distances and the actions of any single entity can significantly impact others. Although communication, both voice and data, is very important in normal operations, during a crisis situation it is absolutely critical.[255]

Where the CATF Report assumes that a Severe Event will degrade communications, the SIRTF Report lays out the challenge it poses and the preparations that BPS operators will need to make in order to carry out necessary continuous communications (i.e., going for

254. SIRTF REPORT, *supra* note 13, at 27.

255. *Id.* at 39 (footnote omitted).

days or even hours without communications must not be allowed to happen). The SIRTF Report states: "During a Severe Event communications will be degraded to some extent, and entities may experience the complete loss of normal communications. Despite this, operating entities must strive to continue to monitor the system and direct operations at all times regardless of circumstances."[256]

Since "load shedding" will be needed in order to manage "graceful degradation" of electric power from the large interconnections into surviving, smaller, potentially isolated "electric islands" (or widely distributed electric archipelagos), the BPS operators will also need to make sure that they maintain situational awareness over such "islands."[257] That, in turn, requires that they prepare to salvage or jury-rig communications that permit the requisite internal system information updates and external sharing of information with customers, suppliers, first responders, and the federal government (whose role, unfortunately, the CATF and SIRTF Reports do not attempt to illuminate or explore).[258]

A BPS operator's loss of communications, both within its organization and with other organizations, appears a foregone conclusion in the CATF and SIRTF Reports.[259] The CATF Report presumes loss of communications (and of long lead-time equipment), as evident in this passage on the challenges of restoration of impaired or disrupted situational awareness after a Severe Event:

> Restoration of situational awareness may have to be manually implemented with staff physically stationed at key locations until communication with monitoring equipment and associated telemetry is restored. Restoration may also involve repair or replacement of parts suffering physical damage from a cyber event. Some of these may require long lead times for replacement due to supply chain or skilled installation workforce availability issues.[260]

256. *Id.*
257. *Id.* at 33.
258. *Id.* at 26.
259. CATF REPORT, *supra* note 13, at 2 (Executive Summary).
260. *Id.*

The SIRTF Report notes, of course, that the loss of communications may derive from disruptions of the BPS, damage to telecommunications, or communications overload.[261] Thus, the SIRTF Report assumes degradation of communications as a result of a Severe Event for a variety of reasons, including:

- Loss of BPS power supply to telecommunications facilities;
- Physical damage to telecommunications facilities;
- The user volume of communications exceeds the capacity of communications facilities, especially cellular and satellite telephone networks.[262]

Of those causes, the one most easily overlooked is the third: communications overload.[263] And it is the one that many in the Northeast have experienced during and after emergencies,[264] as explained in an August 2011 *Scientific American* article:

> Anyone in the eastern portion of the U.S. this week who was forced to evacuate an office, home or school following Tuesday's magnitude 5.8 earthquake soon noticed that cell phone service was spotty or, in many cases, nonexistent. For New Yorkers herded outside of their skyscrapers and into the streets, it was a communication blackout reminiscent of (although of course not the same as) the 9/11 terrorist attacks. In both situations, mobile phone users were unable to connect to the cell network to communicate with loved ones.
>
> Whereas the 9/11 cell phone outage was the result of many factors—including the downing of cell phone towers—this week's problems (though brief) were caused purely by volume. Countless cell phone users were fighting for limited access, leaving most without service.[265]

The overload problem will be exacerbated by the emerging plans of the large telecommunications providers (e.g., Verizon and

261. SIRTF REPORT, *supra* note 13, at 39.

262. *Id.*

263. During emergency situations, many more people attempt to make telephone calls on wireless networks than normal conditions, overloading cell towers and network switches.

264. Larry Greenemeier, *Can Mobile Phone Networks Be Improved to Better Cope with Emergencies?*, SCI. AM. (Aug. 26, 2011), *available at* http://www.scientificamerican.com/article.cfm?id=smart-phone-emergency.

265. *Id.*

AT&T) to refuse to replace or rebuild landlines destroyed by storms (such as Hurricane Sandy) and to install in their place wireless or fiber-optic—less reliable—service "even though the new services often fail during a blackout."[266] The difference in reliability between wireless or fiber optics and landlines is substantial and will burden any BPS or other critical infrastructure operator whose landline service has been removed or replaced.[267]

Traditional copper landlines use electric pulses to carry voice and data signals over a metal wire, which also carries power, so the phone works during a blackout. Fiber-optic lines are made of a thin glass filament and transmit voice and data at high speeds using pulses of light, but they cannot carry electricity and do not work during a power failure without a battery. Cable television wires, which can also transmit telephone service, are made of copper, but they require a modem powered by electricity. Even cell phones require power at the cell tower—something that was knocked out during Sandy.[268]

To our knowledge, most BPS emergency and contingency plans and preparations were derived from operations based on—and continue to presume and rely ultimately on the reliability of—land line telecommunications for voice and data.[269] The general

266. Edward Wyatt, *On a New Jersey Islet, Twilight of the Landline*, N.Y. TIMES, Oct. 15, 2013, at B1, *available at* 2013 WLNR 25792525.

267. *See id.* Note also that in some instances, Verizon is installing a wireless service called "Voice Link" instead of repairing damaged landlines. Voice Link's wireless service will "not work if power fails—a backup battery provides two hours of talking time, hardly reassuring to people battered by Sandy," and

> calls to 911 under normal conditions might not go through because of network congestion. Medical devices that require periodic tests over phone lines, like many pacemakers, cannot transmit over Voice Link. Fax machines do not work over most wireless phone networks . . . . Neither do many home security systems, which depend on a copper phone line to connect to a response center.

Id.

268. *Id.*

269. NERC's emergency operations standard, for example, requires BPS operators to have emergency plans with communications protocols to be used during emergencies, but the standards, plans, and reliability assessment tools appear to assume that conventional, wireless, and satellite communications will be functioning as normal. *See, e.g.*, *Standard EOP-001-0b Emergency Operations Planning*, N. AM. ELECTRIC RELIABILITY CORP. (2011), http://www.nerc.com/pa/Stand/ReliabilityStandards/Reliability%20Standards%20DL/EOP-001-0b.pdf.

public (and probably most boards) view electric outages as posing risks to voice communications; but they probably underestimate the risks to wireless and data communications, which are vital to maintaining situational awareness during and after a Severe Event.[270] Thus, the SIRTF Report, in a rare and emphatic caution, points out: "Effective BPS restoration and continued operation is highly dependent upon the ability to communicate, both voice and data, at all times. The highly interdependent aspect of BPS recovery and the communications infrastructure cannot be over-emphasized."[271]

To address this interdependence of communications after a Severe Event, the SIRTF Report does not recommend BPS owners and operators search for answers in the CIP Standards[272] or in the after-action report from NERC's first sector-specific, large-scale grid security exercise, GridEx 2011.[273] Instead, the SIRTF Report urged

270. *See Surprise! Your High-Tech Home Phone System Could Go Dead in an Emergency*, CONSUMER REP. (Jan. 2012), http://www.consumerreports.org/cro/2012/01/surprise-your-high-tech-home-phone-system-could-go-dead-in-an-emergency/index.htm.

271. SIRTF Report, *supra* note 13, at 62.

272. The SIRTF Report reflects an awareness that the CIP Standards process is flawed by the glacial pace of its progress, by its inconsistent coverage (applying only to identified "critical assets"), by its over-emphasis toward the narrow limits of a compliance culture, by its failure to address any vision of the Severe Event scenario, and by the awkward nature of FERC's limited authority over cybersecurity of the BPS. Such flaws are increasingly the subject of discussion in the federal government as evidenced by the following observations:

> Under section 215 [of the Energy Policy Act of 2005], FERC cannot prescribe its own standards or directly amend NERC's standards . . . . The process of developing these reliability standards is lengthy . . . . It can take NERC six months or longer to respond to FERC's initial order to submit reliability standards. It then takes FERC months to review these proposed standards . . . .
>
> For example, the first critical infrastructure protection (CIP) standards approved by FERC in January 2008 took more than three years for NERC to develop . . . . It subsequently took NERC 43 months to develop and submit the most recent Version 5 of the CIP standards to FERC for approval. Such timeframes are not well suited to address rapidly evolving grid security vulnerabilities.

STAFF OF CONGRESSMEN EDWARD J. MARKEY & HENRY A. WAXMAN, *supra* note 49, at 7.

273. From the after-action report from GridEx 2011, it appears that exercise did not provide the challenges of a Severe Event, but instead revealed the weaknesses in "vertical" information sharing between BPS companies and the regulatory authorities during a cyber attack scenario throughout which

an approach that BPS owners and operators could quickly understand and apply, tailor to their own unique operational environment, and negotiate with telecommunications service providers without undue concern for regulatory oversight and compliance concerns.[274] The recommendations are grounded in common sense practicalities that a BPS board and management would probably find refreshingly clear and appealing because these would allow BPS and telecommunications companies to share their respective worst-case scenario plans and "lessons learned and applied" from the previous experiences that might most closely, albeit imperfectly, approximate Severe Event challenges:

> Entities should work closely with their communications service-providers to better understand mutual dependencies, identify priorities, and seek ways of mitigating the impact of severe disruptions.
>
> • Identify specific interdependencies between telecommunication infrastructure and BPS infrastructure, such as voice and protection circuits, SCADA, remote terminal units and smart grid devices, necessary for BPS operations . . . .

telecommunications appeared to operate reliably. Such an assumption would be unrealistic in a Severe Event exercise, and it is unclear as of this time whether the next GridEx, scheduled for November 2013, will include the Severe Event challenges identified in the CATF and SIRTF Reports. The kind of information sharing problems revealed by GridEx 2011 included:

> The quality of information sharing and reporting to NERC's ES-ISAC [Electricity Sector—Information Sharing and Analysis Center] and relevant government agencies was not as frequent or comprehensive as the communication occurring across the BPS . . . . Despite the assurance that NERC reporting would not be used for compliance purposes, several entities expressed hesitation in sharing sensitive information regarding compromised critical cyber infrastructure. One entity indicated that it was contacting corporate legal for "permission" to report to the ES-ISAC. This *trust deficit* significantly impeded entities' willingness to share information that could have supported the ES-ISAC's role in ensuring grid reliability.

N. AM. ELECTRIC RELIABILITY CORP., 2011 NERC GRID SECURITY EXERCISE: AFTER ACTION REPORT 12 (2012), *available at* http://www.nerc.com/files/NERC_GridEx_AAR_16Mar2012_Final.pdf (emphasis added).

274. SIRTF REPORT, *supra* note 13, at 62.

> - Ensure that critical telecommunications users are registered for priority wireless and land-line services . . . .
> - Identify risks and hazards such as failures, attacks, High Impact Low Frequency Events and/or congestion etc., that could impair the quality of service continuity, readiness, performance and time response of telecommunications.
> - Take mitigation measures . . . .
>
> Consider working with communications service providers to identify which of their facilities are critical to BPS operations. Determine which BPS and distribution facilities supply them and what backup power capacity is in-place (e.g., batteries, standby generators).[275]

While providing guidance for BPS and telecommunications owners and operators to coordinate their Severe Event plans and preparations, the SIRTF Report avoids making the common mistake of thinking that a sensible recommendation will necessarily lead to a satisfactory result.[276] Consistent with the underlying assumption of preparing for successful attacks and their consequences, the SIRTF Report also addresses the preparations that would be needed should telecommunications plans go awry.[277] Personnel need to know what "damage control" actions they should take on their own initiative in the absence of orders from senior management. As the SIRTF Report recommends in its discussion of "Standing Orders for Personnel":

> Standing orders are a prescribed set of instructions for people to take action in the absence of communications or leadership direction. Standing orders could be developed to direct key personnel to report to designated locations following a Severe Event or direct a sub-station technician to clear each bus and open each breaker following a large scale blackout.[278]

275. *Id.* at 62–63.

276. The SIRTF REPORT, for example, observes: "If fuel is not prioritized to communications facilities, the ability to operate portions of the BPS will be severely limited." *Id.* at 74. This is yet another instance in which the SIRTF Report carefully imagines the worst and does not fail to reduce it to its realistic elements and to address those with resourceful and practical recommendations.

277. *Id.* at 44.

278. *Id.*

This is yet another instance in which the SIRTF Report carefully imagines the worst and does not fail to reduce it to its realistic elements and addresses those with resourceful and practical recommendations.

When BPS companies try out and test their Severe Event preparations, they should consider extending the "Standing Orders for Personnel" to incorporate "damage control" training methods used by the U.S. Navy. On submarines, for example, the Navy trains damage control through realistic rehearsals and then runs them again; on the rerun, the crew is told that certain key personnel (officers or NCOs) are incapacitated or dead, and the crew has to perform the "damage control" without communications from leaders and still accomplish the objective of making the right initial decisions and adjusting to potentially deteriorating circumstances.[279]

VII. COUNSEL'S DISCUSSION OF THE SALIENT CYBERSECURITY QUESTIONS WITH A BOARD AND MANAGEMENT

Counsel advising a critical infrastructure board and management on the company's approach to cybersecurity need to be aware that the most serious cyber threats to such companies will often not be those that involve reporting of data breaches (notwithstanding the considerable importance of such incidents and the reporting obligations that they trigger). As the NERC Task Force reports make clear, the most serious cyber threats create "high-impact, low-frequency" risks that the company's operations

279. Although current Navy "damage control" procedures and training are not released to the public, Navy representative statements posted on Navy websites confirm that the Navy "damage control" training emphasizes ensuring that crews have the skills, initiative, and resourcefulness to step in and perform in an emergency if those assigned to such tasks are unavailable. As a statement on one such website explained in 2009 concerning the U.S.S. Wasp's Damage Control Academy (DCA):

> If an emergency happens and you dial 9-1-1, we're the ones who respond," said Damage Controlman 2nd Class (SW/AW) Adrian Edwards, Wasp's DC office work center supervisor. "But we also train the rest of the crew to fight fires because there's always the chance that we could be incapacitated in some way.

Christopher Koons, *Damage Control Academy Provides Vital Training*, U.S. NAVY (Oct. 24, 2009, 11:08 PM), http://www.navy.mil/submit/display.asp?story_id=49222.

will be damaged and disrupted, and that its ability to meet its contractual and regulatory obligations for reliability may be irreparably degraded.[280] Such companies, therefore, find it challenging to hire a Chief Information Security Officer (CISO) who has the necessary qualifications. Candidates with experience and expertise in business information systems will bring that background into a company where it may appear to be the right skill set, but prove to be a liability. Business information system security expertise is not a skill set that can easily be transferred into critical infrastructure operational system security.[281]

Unless the CISO understands the end-to-end features of a critical infrastructure company's operations, such as a BPS running of electricity generation and transmission services, the CISO will tend to make errant assumptions, apply the wrong solutions, overlook critical issues, and, ultimately, fail to address the most serious issues.[282] For those reasons, some BPS companies have decided instead to hire as a CISO an individual who understands the technical side of their operations and to let that individual learn the applicable cybersecurity tools because then there is far less risk of mistakenly thinking that business information security will transfer to operational system security. Counsel needs to realize that to advise such a company, counsel must avoid the same pitfalls and master the operational system of the client company; only then can counsel advise on the applicable cybersecurity issues.

Even then, counsel will find that advising a BPS company or other critical infrastructure company requires a much broader

280. *See* SIRTF REPORT, *supra* note 13, at 1.

281. Put another way, the training needed to operate the BPS generally requires years of education and field experience to understand the control room; SCADA resources; and interconnected generation, transmission, substation, and field circuitry that delivers power throughout the grid under normal circumstances. NERC emphasizes that there is no training that can be offered to an electric system operator on exactly how the system will fail upon a cyber attack as a Severe Impact event from a cyber attack has never happened and the exact mechanisms of such an attack are not yet known. Therefore, operators need to develop a "sixth sense" on how to react to loss of systems and resources based on existing experience and learn to adapt to and execute the attack scenario. *See* CATF REPORT, *supra* note 13, at 16–20. The authors submit that generalized computer security expertise is insufficient especially in the control rooms where critical decisions will need to be made.

282. *See id.*

grasp of technical issues and divergent and conflicting legal standards and norms than when advising on business information system security.[283] And, as explained in the recently published *ABA Cybersecurity Handbook*, counsel needs to know the limits of effective advice while at the same time knowing when to initiate a conversation about cybersecurity in case the client fails to initiate it:

> Such conversations should help counsel bring home to the client the significance of cybersecurity, the threats and risks to it, and the necessity of developing a responsible approach to those threats and risks. Engaging in a give-and-take conversation will lead, with any luck, to a useful joint exploration of what might limit or compromise the client's cybersecurity.
>
> . . . .
>
> Counsel will want to refrain from attempting too much in a conversation about cybersecurity with a client. Averting cyber [security] incidents will probably remain an elusive ideal, and advocating its pursuit will only frustrate everyone involved. Being too prescriptive or dire will usually be counterproductive, and it is important to know why: prescriptive or dire utterances tend to make conversations one-sided. . . .
>
> . . . .
>
> . . . And, as a colleague recently noted, if lawyers, in conversation with clients, give more information than they get, the client will in all likelihood stop listening.[284]

Since the issuance of the EO, boards and management of critical infrastructure companies have not needed counsel to suggest they make cybersecurity a priority on their meeting

283. As we have explained throughout this essay, counsel advising BPS clients only on the EO, PPD-21, and the need to respond to the federal government's requests for implementation of the Framework will miss at least half the issues, and we respectfully submit the same is true for counsel advising critical infrastructure owners and operators in any of the other sectors. Understanding the industry-specific regulatory structure is critical, with the role NERC plays as the ERO and FERC plays as the reviewer, approver and, with NERC, enforcer of CIP standards. These collectively make the Framework, EO, and PPD-21 important resources, but they are not controlling of the regulatory responsibilities for BPS owners and operators.

284. Roland L. Trope, *Duty to Advise Clients Concerning Use of Cyber and Other Digital Technologies*, *in* THE ABA CYBERSECURITY HANDBOOK 81, 81, 96 (Jill D. Rhodes & Vincent I. Polley eds., 2013).

agendas. Well-managed companies will have made cybersecurity a high priority. However, the issuance of the EO and PPD-21 has created more confusion than clarity.[285] One part of the confusion derives from the EO's invocation of a national security threat and the President's low-key mention of it during the State of the Union speech the same day. Another part of the confusion derives from the attention attracted by the Edward Snowden NSA surveillance disclosures, which have distracted attention away from the White House's efforts, through the EO and Cybersecurity Framework, to coax critical infrastructure companies to improve cybersecurity.[286] In fact, the reportage and discussion of the Snowden disclosures have created a disruptive "noise" behind the EO that has severely impeded its "signal."[287]

285. *See supra* note 122 and accompanying text.

286. Recent remarks by former National Security Agency Chief General Michael Hayden evidence that the Snowden disclosures have created a serious distraction from cybersecurity efforts:

> In terms of the broad cyber effort—as concerned as I am about the government shutdown, I'm more concerned about the byproducts of the Snowden revelations. . . .
>
> But with the Snowden revelations, frankly, quite a bit sensationalized—it's clear to me that there's a very low probability we're going to get any cyber legislation out of this Congress. We need cyber legislation. We need to think through how it is we want to defend ourselves. The way I put it is, "what is it we want our government to do in the cyber domain" and "what is it we'll let our government do." And I'm afraid this whole kerfuffle since June has just poisoned that water.

Brian Fung, *Former NSA Chief: NSA and U.S. Cyber Command Are Now 'Indistinguishable,'* WASH. POST (Oct. 23, 2013), 2013 WLNR 26623383.

287. As explained by Professors Pierce and Noll,

> In long-distance calls you may hear a hissing or slushing sound even when no one is speaking. The sound is caused by random electric signals that are unavoidably added to the electric speech signal when it is sent over telephone circuits. . . . If P_s is the signal power and P_N is the noise power, the signal-to-noise ratio is expressed in deciBels is 10 $\log_{10}$ (Ps/Pn) dB. A speech signal-to-noise ratio of 60 dB or more is really high fidelity. A signal-to-noise ratio of 20 dB is very intelligible but noticeably noisy. Between 10 and 1 dB the signal becomes nearly unintelligible. . . .
>
> . . . .
>
> If the radio-frequency signal-to-noise ratio is inadequate, the receiver can make mistakes in interpreting the binary digits, and the recovered signal suffers huge errors.

JOHN R. PIERCE & A. MICHAEL NOLL, SIGNALS: THE SCIENCE OF TELECOMMUNICATIONS

But boards and management of critical infrastructure companies appear to have been most concerned this year with the divergent claims and objectives of cybersecurity initiatives that attempt to demand corporate attention. Having reviewed some representative samples of those initiatives, we are in a position to address the five questions mentioned earlier. Those questions reflect the issues on which boards and management appear to be most frequently asking for guidance from counsel at this juncture—in the fall of 2013. The questions arise in response to the president's declaration in the EO that the threats of cyber attacks on critical infrastructure pose a challenge to U.S. national security and in response to the quite different set of threats of kinetic cyber attacks identified in the NERC's Task Force reports. The answers we will explore will attempt to provide the breadth of inputs of the legal, operational, and cybersecurity perspective that may be requested of counsel and that counsel would, in any event, attempt to combine in their responses in discussion with a critical infrastructure board and management. We will also try in this

28–29, 81 (1990).

> As is well explained by Jack Goldsmith:
>
> A major challenge for the government, and one it has not yet figured out how to accomplish, is to give the NSA wider latitude to monitor private networks and respond to the most serious computer threats while at the same time credibly establishing that the agency is not doing awful things with its access to private communications. Such credibility is hard to establish, and so the government will likely hold back until we suffer a catastrophic cyber attack. . . .
>
> I still think this holds true, but would modify it a bit. NSA won't be able to do the things that General Alexander wants to do in the private network until the lights go out for a week, or some similar such catastrophe.

Jack Goldsmith, *The Snowden Revelations and Cybersecurity*, LAWFARE (Aug. 14, 2013, 7:03 AM), http://www.lawfareblog.com/2013/08/the-snowden-revelations-and-cybersecurity/ (quoting Jack Goldsmith, *The New Vulnerability*, NEW REPUBLIC, June 7, 2010, at 21, *available at* LEXIS). The Snowden disclosures have not only prompted protests from governments friendly to the United States, but led President Obama to launch two intelligence reviews (one internal, one external): "Those reviews have taken on growing international significance in recent weeks as top administration officials repeatedly cite them in response to anger from European leaders following revelations about Ms. Merkel and about surveillance of phone calls in France." Siobhan Gorman & Adam Entous, *Obama Unaware as U.S. Spied on World Leaders: Officials*, WALL ST. J., Oct. 28, 2013, at A1, *available at* LEXIS.

discussion to assist boards in assessing the extent to which they may have to choose between the divergent objectives and recommendations expressed, on one hand, in the EO (and its initiatives), and on the other hand, in the NERC Task Force reports (and their recommendations).

A. *"How seriously should our company take the government's declaration of this cyber threat?"*

There are really three issues that this question raises. Each issue concerns a different declaration by the federal government of a cyber threat and each requires an answer to an underlying question. Each underlying question requires companies to identify who is *responsible for addressing the threat* by making the requisite preparations—to defend against the threat, respond to contain and mitigate the damage from it, and manage the recovery of services degraded by it, to whatever extent and for however long.

1. Threat Identified in the EO

The first declaration occurred in the EO and is expressed in terms that identify it as current, direct, and serious: "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The *cyber threat to critical infrastructure* continues to grow and *represents one of the most serious national security challenges* we must confront."[288] Given the EO's limited scope of authority, the pronoun "we" might arguably refer only to the executive branch. That reading is far too literal and narrow, particularly in light of the EO's directions to increase information sharing and to develop the Framework. Both of those initiatives aim at motivating, coaxing, and persuading private industry—and critical infrastructure owners and operators in particular—to take actions to enhance their cybersecurity because the EO is not speaking of a threat to the federal government nor generally to the nation, but emphasizes it is a "threat to critical infrastructure."[289]

As noted earlier, responsibility for protecting a critical infrastructure sector rests with the companies that operate it, and it is the responsibility of each such company to protect itself. Should

288. Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,739 (Feb. 19, 2013) (emphasis added).

289. *Id.*

its management be negligent in identifying and addressing a risk to the enterprise, management and the board overseeing its actions bear the responsibility. So, with respect to the EO's identification of the "cyber threat to critical infrastructure"[290] the EO makes clear: it is "one of the most serious national security challenges" that confronts each sector of critical infrastructure, each company operator within a sector, and, ultimately, each such company's board and management.[291] To treat that cyber threat as anything less than one of the highest priorities for a board and management after the issuance of the EO exposes the board to the risk of failing to fulfill its fiduciary duties for the enterprise.

2. Threat Identified in Catastrophic Target Notice

The second federal declaration of a threat will be issued in accordance with the EO's direction that certain critical infrastructure companies receive what we have referred to as a Catastrophic Target Notice.[292] That Notice will inform a critical infrastructure company that the federal government has determined that, if such company is damaged or otherwise affected by a "cybersecurity incident," it could "reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[293] This second kind of cyber threat is a subset of the first and, as such, it too is current, direct, and serious. It emphasizes implicitly that the recipient has been put on notice that it now has knowledge of the widespread damage that could result if its *operations* are damaged and degraded by a cyber attack.

In short, a Catastrophic Target Notice tells a company that if the current cyber threat to the nation's critical infrastructure targets your operations, the damages will not be to you alone and thus your preparations for such cyber attacks should not be confined solely to protecting your operations. Instead, your company has much broader responsibilities to avert, limit, or mitigate the consequences that could flow from a degradation of its operations. Thus, a cyber threat to you poses a risk of "catastrophic

290. *Id.*
291. *Id.*
292. *See supra* Part V.A.2.
293. Exec. Order No. 13,636, 78 Fed. Reg. at 11,742.

regional or national effects on public health or safety, economic security, or national security."[294] Neither the EO nor the Catastrophic Target Notices issued under its authority impose such responsibilities (that could only occur through a federal statute). However, once a critical infrastructure company receives such a Notice, its board and management must take it, and the risks it identifies, seriously.

The determination to issue a company a Catastrophic Target Notice is made by the DHS, not by a mere outside consultant. The determination is made within the context of a declared threat to national security. From February 2013 onwards, company boards and management have been aware of the possibility of receiving such a Catastrophic Target Notice. Thus, they have arguably had ample time to deliberate carefully and decide what preparations should be made in order to address such risks, particularly since most candidates for receipt of a Catastrophic Target Notice probably expect to receive it—and that would surely include all of the major BPS owners and operators in the United States.

Failure to take seriously such a credibly identified risk, and one of expressly "catastrophic" magnitude, could expose a company and its board and management to regulatory sanctions and lawsuits. This is particularly true if a cyber attack did indeed damage the company's operations, particularly if a plaintiff or a post-event regulator investigation discovered evidence suggesting that "but for" the company's failure to take the Notice seriously and act responsibly to reduce the risk, the damage would have been averted or substantially less extensive, and recovery from it would have occurred more quickly and at less expense to all the regionally or nationally affected parties.

3. Threat Identified in Imminent Target Notice

The third federal declaration of a threat will be issued in accordance with the EO's direction that certain critical infrastructure companies receive what we have referred to as an Imminent Target Notice.[295] It will inform the recipient that it is one of the targets of a planned attack against the U.S. homeland. The Imminent Target Notice is thus expressed as direct, serious, and, in

294. *Id.*

295. *See supra* Part V.A.3.

this instance, imminent. Companies may receive such notices with little or almost no time to make responsible preparations. Here again, however, any critical infrastructure company has been on notice, since the February 2013 issuance of the EO, that it could receive such a Notice.

Thus, such companies have had time to deliberate carefully as to what preparations would need to be made in response to a serious threat supported, not by rumors or news media reports, but by credible federal cyber intelligence. In the face of what purports to be a notice of an extraordinary and imminent threat, no board or management will find much protection from liability in arguing that the brief period between the delivery of the Imminent Target Notice and the start of the cyber attack left the company insufficient time to make plans and enhance preparations. It would not be persuasive because the company had several months during which it knew it might receive such a Notice and could have made appropriate plans and preparations during that time.

4. Viewing the Three Threats Together

Now consider the position of a board and management asking counsel: how seriously should we take each of these three threats? Counsel should not only be addressing them separately as we have done here, but should also point out that all critical infrastructure companies have received the first threat notice (contained in the EO), and many such companies should anticipate that they will receive *both* of the other threat notices—Catastrophic Target Notice and Imminent Target Notice. In that instance, it would be prudent for the company and its board and management to recognize that they now have new corporate cybersecurity responsibilities, each defined by the respective federal threat notices, and each enhancing the extent to which such threats should be taken seriously and addressed accordingly. In doing so, it will be important to understand the implicit "forewarned-forearmed" strategy of the EO and its information-sharing Notices:

> [T]he strategy implicit in the EO's use of notices is the proverbial "forewarned—forearmed." Receipt of a notice will narrow owner-operator alternatives. Inaction is unjustifiable; superficial action, when viewed by judges, risks being deemed negligent or recklessly indifferent to clear government warnings. Notices will make it difficult to excuse postponing investments in cybersecurity and

> disaster recovery as courts might view receipt of a notice as putting the onus on owners and operators to justify what they subsequently did and did not do. If a head-in-the-sand approach to cybersecurity prevailed at a company, that approach will probably be relinquished upon delivery of DHS notices.[296]

5. Counsel's Recommendations

For the reasons given, each threat warrants serious urgent attention by management. The board, for the same reasons, may decide to assign certain board members or a committee to maintain closer than usual oversight of management's decisions on preparations to be made. The board should be informed of the intended preparations, the priorities among them in view of time and budget constraints, and the progress of their implementation and request timely reassessments based on updates of the preparations' progress and of additional threat information. The need for closer and more frequent monitoring of these activities is driven by the probability that before and during a cyber attack, the emergence of, and changes in, the relevant facts will be quick and frequent.[297]

Similarly, the need for crucial decisions and reassessment of plans, preparations, and actions will arise abruptly and without any sense of a schedule or cycle. Unlike a hurricane threat to a region's BPS operations, in the event a cyber threat or attack arises, there will be neither gradual, orderly updates of the approaching threat nor ever-increasingly accurate predictions of the timing of its arrival and the extent of its impact. Everything that management addresses and that the board may want to oversee will move with accelerated rapidity, and there will be unpredictable developments that may necessitate considerable changes in approach, plans, preparations, and actions. Maintaining orderly communications, situational awareness, and calm decision making will be a high priority to prevent the adversaries from causing a company's crisis management from undermining its own efforts to protect the

296. Trope & Humes, *supra* note 152, at 4–5.

297. For recommended response actions during or after a cyber attack with respect to information sharing, see CATF REPORT, *supra* note 13, at 59 ("System Operations and ESP Monitoring personnel should have frequent conference calls to correlate monitored ESP activity and system operations abnormal readings.").

enterprise. In short, achievement of "graceful degradation" of operations will require that management maintain order despite the cyber attack's attempts to destabilize, disrupt, confuse, and cause chaos, panic, and self-sabotaging mistakes.

Because a Severe Event caused by a kinetic cyber attack will take a critical infrastructure company and its board and management far beyond their "comfort zone" into experiences for which no prior experience will provide a reliable guide, it is important for counsel to encourage the board and management to understand those challenges. As a result, counsel should put more than the usual emphasis on promptly starting and expeditiously completing preparations for handling the Severe Event and the New Normal that follows from it. Among the earliest of those preparations, however, should be efforts to ensure that the company is *ready to receive and responsibly handle* each of the federal government's threat notices.[298] The following questions, among others, will need to be addressed in advance of receiving a Catastrophic Target Notice and/or Imminent Target Notice:

- Who in the company will be designated to receive and initially review any Notices received from DHS, regardless of the day and hour they are received?
- Who else in the company has a "need to know" the receipt and contents of each Notice?

298. Recall that the federal government will also be sharing "classified" threat information through third party vendors, but we have omitted discussion of those in this section because the procedures and details remain, to date, undisclosed. But no company can receive such information unless it has applied for and obtained clearances for its personnel (and preferably at least one member of the board and general counsel) and has ensured that such information is protected in accordance with applicable statutes and regulations.

The Department of the Treasury, in a recent report to the president, emphasized the preparations that critical infrastructure companies would need to make to participate fully in the information sharing authorized by the EO. "In order to fully participate in this program, critical infrastructure organizations must have the capability to send, receive, and act upon information about cyber threats and vulnerabilities." DEP'T OF TREASURY, REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636, at 9 (2013), *available at* http://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf.

- Who has the authority in the company to make, or coordinate the making of, decisions concerning the company's response(s) to each Notice?
- Has the company adopted a set of formal procedures for ensuring that receipt of each Notice, and the information contained in each, *is protected from unauthorized disclosure outside the company and unauthorized access within the company*?
- Where will the company store such Notices (if in hardcopy and if in digital copy) so that cyber adversaries cannot gain access to that information through the Internet or through the company's business information systems?

  Note: In addressing this question, assume that adversaries may already have injected malware into the company's networks that could exfiltrate such information and exploit it to the company's disadvantage during a planned cyber attack.
- Does the company have plans and preparations ready to implement in the event it receives a Catastrophic Target Notice and to act responsibly and quickly to reduce the risks identified in such Notice?
- Does the company have plans and preparations ready to implement in the event it receives an Imminent Target Notice and needs to act responsibly and quickly in anticipation of the cyber attack identified in such Notice?
- If the company has made plans and preparations for receipt of a Catastrophic Target Notice or Imminent Target Notice, has it based them on a cyber attack that produces a Severe Event (requiring a "graceful degradation" of operations)?
- If so, has it also based them on an attack that results in a New Normal (requiring months of recovery to restored reduced operations)?

Thus, counsel will be seeking to ensure that the focus is on the most serious of cyber threats to a critical infrastructure company, which is the issue addressed by the next question.

B. "If the cyber threat poses a serious risk to our company, is the main risk to our company's business information systems or to its operation and control systems?"

1. The Ultimate Target of Cyber Attacks on Critical Infrastructure

The EO fails to make explicit whether the "repeated cyber intrusions" it mentions involve attacks to critical infrastructure on the company's business information systems, its operational systems, or both.[299] One can, however, draw the following reasonable inferences from the EO:[300]

- If the ultimate objective of the "cyber intrusions" was only to exfiltrate business information, the resulting damage to critical infrastructure would not, in most instances, put national security at risk or cause "catastrophic" effects regionally or nationally.
- "Cyber intrusions" that target business information systems may be part of a larger intelligence gathering effort to seek data, such as testing awareness or response capabilities that can be used to design and execute an attack against a company's operational systems.
- For a cyber attack to create a national security risk to critical infrastructure and a risk of "catastrophic" effects regionally or nationally, the objective will almost certainly be to damage and disrupt the target's operational systems.

2. Counsel's Recommendations

For those reasons, counsel will probably need to advise a critical infrastructure client that its response to the cyber threats identified by the federal government should be to treat its operational systems as the "main risk" and, for that reason, ensure that the business information systems are kept absolutely separate from the company's operational systems. That can be done in part by "air gapping"[301] the operational systems of computers and

299. *See* Exec. Order No. 13,636, 78 Fed. Reg. at 11,742.

300. *Id.*

301. Air gapping is a physical separation of a system, such as a control room, from the Internet or any means of connecting to the Internet. NERC's CATF Report indicates that reliance on air gapping alone offers a false sense of security as attacks have been launched on air-gapped systems through memory sticks or

SCADA interfaces or by inserting digital diodes[302] in each two-way communications link. What is crucial is for two things to be kept inviolate from unauthorized access or release: the controls and monitors of the operational systems *and* the security plans (physical and cyber safeguards, incident responses, recovery plans, etc.).

Once the operational systems become the focus of protective measures, the next issue becomes how extensively they need to be protected, which is the subject of the next question.

C. *"If the main risk of the cyber threat is to our company's operation and control systems, how comprehensive should our company's preparations be?"*

1. *Interpreting the Concept of "Comprehensive Preparations"*

This question is probably the hardest for any company to answer. Even if companies could be made *invulnerable* to cyber attack, the cost to accomplish invulnerability would be prohibitive. Additionally, the invulnerability would only be temporary in the rapidly evolving world of cyber threats. Moreover, few, if any, cybersecurity experts believe that any company can be made invulnerable to cyber attack.[303] The White House initiatives do not

other devices inserted into USB drives, for example. *See* CATF REPORT, *supra* note 13, at 71.

302. Digital diodes, also known as data diodes, are another part of a network perimeter defense designed to stop a cyber intrusion into a control center or other cyber asset by using a combination of routable or non-routable protocols in a communications link to achieve isolation. *See id.* at 65.

303. Dating back at least to 2007, cybersecurity experts have viewed making a company invulnerable against a targeted cyber attack as an unattainable goal. Expressions of that view appear in assessments ranging from 2008 through the present. *See, e.g.*, BRITISH-N. AM. COMMITTEE, CYBER ATTACK: A RISK MANAGEMENT PRIMER FOR CEOS AND DIRECTORS 1 (2007), *available at* http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=4888caa0-b3db-1461-98b9-e20e7b9c13d4&lng=en&id=111174 ("No business, government, nongovernmental, or other organization of whatever size is invulnerable to cyber attacks."); VERIZON BUS. RISK TEAM, 2008 DATA BREACH INVESTIGATIONS REPORT 18 (2008), *available at* http://www.verizonenterprise.com/resources/security/databreachreport.pdf ("[A]n organization singled out by an attacker with sufficient resources will find it difficult to mount an adequate defense."); Taylor Armerding, *Best Defense Against Cyberattacks Is Good Offense, Says Former DHS Official*, CSO (Sept. 26, 2012), http://www.csoonline.com/article/717331/best-defense-against-cyberattacks-is-good-offense-says-former-dhs-official ("We will never defend

seek that.[304] Instead, as we noted earlier, the White House seeks to have critical infrastructure companies improve their cyber hygiene in order for such companies to cease being easy prey for cyber adversaries.[305] That minimal objective is achievable, but it nonetheless requires extraordinarily effective training of personnel who will otherwise continue to make mistakes when subject to "social engineering" tricks that invite them to click on a hyperlink or open a file and, thereby, grant an adversary's malware easy access to their company's computers. So with respect to the White House objectives, the effort needs to be fairly comprehensive. Training personnel in good cyber hygiene will require efforts that are both comprehensive (including board members and senior management) and relentless. The efforts, in other words, must be capable of addressing the magnitude and level of persistence that serious and sophisticated adversaries will bring against critical infrastructure. The adversary will relentlessly probe for vulnerabilities. And, as a result, the adversary may find an easy way to execute an intelligence intrusion, a massive data exfiltration, and an embedding of worms capable of damaging operational equipment. Companies need to expand their preparations and training to prevent conduct that will otherwise facilitate an adversary in gaining attack intelligence, finding vulnerabilities through which to inject an attack, and carrying out its damaging exploits.

2. Counsel's Recommendations

Having made allowance for efforts to cooperate with the White House's initiatives, we think, in light of the foregoing discussion, a company is best served by directing most of its resources and

our way out of the current cybersecurity crisis. That's because putting all the burden of preventing crime on the victim rarely succeeds." (quoting Stewart Baker, *Rethinking Cybersecurity and the Role of the Private Sector*, STEPTOE CYBERBLOG (Sept. 19, 2012), http://www.steptoecyberblog.com/2012/09/19/rethinking-cybersecurity-retribution-and-the-role-of-the-private-sector/)).

304. *See* Exec. Order No. 13,636, 78 Fed. Reg. at 11,739 (Feb. 19. 2013) ("It is the policy of the United States to *enhance the security and resilience* of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." (emphasis added)).

305. *See supra* notes 228, 292 and accompanying text.

thoughtful planning to preparations for what appears to be inevitable: the launching of a cyber attack that targets critical infrastructure and that succeeds in causing enough damage and disruption to result in a Severe Event and a New Normal. Preparations, therefore, must focus on resilience—how efficiently and effectively the cyber critical asset operator can recover and adjust to the New Normal.[306]

With those preparations as the highest-priority objective, the issue of "comprehensive" actually becomes easier to answer. Most of the hard work of preparing for a Severe Event is not cost intensive (especially when compared with the costs of procuring crucial BPS equipment such as transformers).[307] It requires carefully thought-out plans and preparations, "red-teaming"[308] the successive versions, and devoting time for realistic training that includes depriving personnel of leadership and directions so that they will be capable nonetheless of taking the right actions at the start and can carry out their duties for prolonged periods on their own initiatives.

Cost-intensive issues will arise when, for example, a BPS company realizes that a cyber adversary may damage equipment that is no longer manufactured in North America and that procurement of replacement spare parts or new units has a lead time of six months or longer. Boards and management will need to address questions such as:

306. Conceptually, the issue is the same as storm preparation and response. No company can stop a natural disaster, such as a hurricane, tornado, or wild fire. The issue for storm preparation and response, like a cyber attack, is resilience—how quickly and efficiently the company can recover and restore service to normal.

307. Among the many recommendations of the NERC SIRTF Report, one stands out with respect to planning for major equipment replacements that may be needed in response to a cyber attack, including transformers and other equipment that are costly and require long lead times. The SIRTF Report recommends that companies conduct short- and long-term system planning exercises to explore recommended strategies that might include temporary alternative equipment interoperability options to speed system restoration when certain equipment might be unavailable. SIRTF REPORT, *supra* note 13, at 49.

308. In current energy industry vernacular, use of the term "blind" or "red-team" testing is typically conducted by people who are given no information at the start, with the goal of seeing if security perimeters can be breached by trial and error, brute force, stealth, masquerade, etc.

- Should the company revise its budget (and will regulators allow the cost recovery in rates) for maintaining an inventory of critical spares and units (such as heavy transformers) in order to reduce the time needed to restore operations after a Severe Event and during a New Normal of degraded operations?
- If the company (and its regulators) would find such costs unacceptable, can it enter into cost-sharing arrangements with other companies in its sector that would make procurement of long lead-time spares and units affordable and available when needed after a Severe Event?
- Can the company enter into agreements with offshore manufacturers of critical parts and units that will allow it to have emergency orders filled on an expedited schedule that would also help the company manage the New Normal with enhanced predictability?

That such cost issues could arise and make a substantial difference to the duration of a company's recovery efforts after a Severe Event suggests also that some companies may find themselves in financial distress during that period.[309] It would therefore be prudent for the board and management to address the need for extraordinary contingency financing on the occurrence of a Severe Event.

Lastly, when counsel checks to see if the company's response will be comprehensive enough to address the significant legal risks, attention should be given in advance to whether receipt of a Catastrophic Target Notice or Imminent Target Notice might trigger duties to report their receipt to third parties (e.g., customers, suppliers, lenders, and insurers). Companies will need to review relevant agreements and may want to negotiate amendments to exclude these Notices as in most instances they were not contemplated when executing such agreements.

309. A severe event will also likely impact critical infrastructure companies in the banking sector, which could complicate the financial stresses on BPS owners and operators. The financial security of counter-parties transacting in wholesale power transactions could become impaired and cause cascading effects on critical infrastructure owners and operators to lose ready-access to banking support or their counter-parties' access to credit support.

D. "What priority and urgency should our company give to completing those preparations?"

1. Events that Have Obscured the Need to Proceed Urgently

This is probably the easiest question, but we include it because events since the issuance of the EO have impeded its implementation in ways that the White House could not have imagined and appears to have been unable to overcome. The result is that much of the "signal" that the EO may have tried to transmit and continue transmitting throughout the nation's critical infrastructure communities has been largely drowned out by extraordinarily distracting "noise" and "cross-talk." Instead of the subsequent months evidencing a growing awareness and intention to address the threats identified by the EO, the Catastrophic Target Notices, and the Imminent Target Notices—or those identified by NERC's CATF and SIRTF Reports—owners and operators have found the media and public discourse focused on other issues, including:

- The Snowden disclosures,
- Debate over the extent of NSA domestic surveillance,
- Protests from allies in response to disclosures of U.S. cyber surveillance,
- Congressional and White House impasse over the budget leading to a federal government "shut down," and
- An even more serious impasse over raising the debt ceiling.

These issues have claimed the attention of critical infrastructure companies because each has either drawn attention away from the urgent need to improve cybersecurity or has required boards and management to address the risks that the federal government crises were creating and could create to immediate and long-term business planning.

2. Counsel's Recommendations

Because the "signal-to-noise" ratio has been so poor during the months following the issuance of the EO and since there has been little attention given to the CATF and SIRTF Reports even by some of the largest BPS companies, counsel should probably be advising BPS and other critical infrastructure companies that cybersecurity improvements and preparations for Severe Events should be

treated as among a company's highest priorities and addressed urgently. Furthermore, boards that have not yet actively discussed the cybersecurity issues would benefit from active discussions with counsel on the issues. Otherwise, the evident complacency that preceded and prompted the issuance of the EO will lull critical infrastructure companies into believing that the warnings are not serious, that the threats are exaggerated, and that the demonstrated U.S. capabilities to conduct cyber surveillance will somehow work as a deterrent or defense against adversaries planning cyber attacks and conducting pre-attack surveillance.

Such assumptions put a company in the worst of all positions: it will have received credible warnings of serious threats, it will have had time to make responsible preparations, and it will have failed to act in a timely or effective manner. That raises the company's exposure to post-attack liability and reputational damage while wasting the company's opportunity to avert such risks to its enterprise and operations. It also raises the final issue in this discussion—the standard by which a company's responses to the threats identified by the White House and NERC's CATF and SIRTF Reports will be judged.

E. "In the absence of a uniform federal or state standard for critical infrastructure cybersecurity, by what standard will our response to this cyber threat ultimately be judged?"

1. The "Hurricane Sandy" Test for Critical Infrastructure Responses

Among the multiple applicable standards by which a critical infrastructure company could be judged for its response to notice (formal or informal) and foreseeable risk of cyber threats, we think the most important will be what we would refer to as the "Hurricane Sandy" test or standard.

Owners and operators of BPS and telecommunications companies (and some other critical infrastructure companies) have regulatory standards that they may fail to comply with and by which they may be judged. Typically, for example, electric utilities are required by statute to provide safe, adequate, and reliable service. However, when "high-impact, low-frequency" events paralyze critical infrastructure in a region—as occurred during and after

Hurricane Sandy[310]—there will often be little criticism directed at such companies for the extent to which the storm and the storm

310. As reported a year after Sandy struck, *The Economist* provided a post-storm damage assessment and contrasted it favorably with the recovery efforts by owners and operators of energy and telecommunications companies. *The Economist*'s account suggests that the public—and the media—have judged such owners and operators, not by the damage that the storm inflicted, but by their preparedness to manage the recovery efforts—and by their willingness to invest heavily in preparations that reflect the "lessons learned" from this "high impact, low frequency" event:

> [Forty-four] New Yorkers [were] killed during the storm. Most drowned in the surge which covered *nearly a fifth of the city's land*. Much of the city was in darkness for days, including a lot of Manhattan. Subway tunnels were filled with water and 150,000 homes were damaged across the five boroughs. More than 125 homes burnt to the ground in Breezy Point . . . . The damage across the city was pervasive and extensive.
>
> Yet New Yorkers are resilient. . . . Very quickly the city set up its Rapid Repairs programme [sic], which restored heat and power to 54,000 people and got them back into their homes. . . . Since the storm, the city has begun or completed more than $1 billion worth of Sandy response-and-recovery work. . . .
>
> . . . .
>
> Utilities such as Con Edison and Verizon are also significantly strengthening their kit. Con Edison, an energy company, intends to invest $1 billion in storm-protection measures over the next four years. It is building flood barriers and gates as well as installing "smart" switches to isolate damaged equipment. Verizon, a telecoms giant has speeded up a switch to water-resistant fibre-optics [sic] from copper lines, which should reduce the chance of communications blackouts.

Hurricane Sandy One Year On: Stronger Than the Storm, ECONOMIST, Oct. 19, 2013, at 36, *available at* 2013 WLNR 26139202 (emphasis added).

Note, however, that *The Economist*'s account may be making a seriously inaccurate statement when it observes, reassuringly, that Verizon's replacement of copper wires with fiber-optics cable will "reduce the risks of communications blackouts." *Id.* On the contrary, as we noted earlier, recent reports make clear that the switch to fiber-optics will render communications *less reliable*. This is an example of an all-too-typical instance of a new technology offered for its benefits without adequately addressing the drawbacks, or concealing them from the public because the owners and operators of the critical infrastructure find the deployment of the new technology will enable them to reap larger profits, in part justified by the promise of improvements that are, however, illusory:

> Traditional copper landlines use electric pulses to carry voice and data signals over a metal wire, which also carries power, so the phone works during a blackout. Fiber-optic lines are made of a thin glass filament and transmit voice and data at high speeds using pulses of light, but they

surge disrupted electric power and telephone communications. No one blames local BPS companies for the hurricane; for its chance intersection with the coasts of New York, New Jersey, and Connecticut; or for the widespread outages, loss of heat, loss of water, and loss of control of sewage directly caused by the storm surge. Regulators, politicians, the media, and the general populace accepted that "these things happen" and when they do on this scale, there is little any critical infrastructure company can do to avert them.[311] Severe Events caused by a cyber attack will undoubtedly be viewed with much the same tolerance for failure to withstand the brute force of the attack or to have sufficient resilience to avoid any disruption of operations and degradation of services.

The crucial element that we refer to here as the "Hurricane Sandy" test—the tendency for customers, regulators, governments, and the media to judge electric power companies by their readiness to manage an orderly and reasonably prompt restoration of service to customers—is not limited to the North American cultures and political systems. A similar emphasis on readiness and preparations for handling severe disruptions to major sections of a nation's electric grid can be seen in the Report of the Enquiry Committee investigating the grid disturbance in northern India that occurred on July 30, 2012, and the even more widespread grid disturbance that occurred the following day in the northern, eastern, and northeastern region of India ("India Grid Disturbance Report").[312]

> cannot carry electricity and so do not work during a power failure without a battery.

Wyatt, *supra* note 267.

311. *See e.g.*, PUB. UTIL. REGULATORY AUTH., STATE OF CONN., DOCKET NO. 12-11-07, PURA INVESTIGATION INTO THE PERFORMANCE OF CONNECTICUT'S ELECTRIC DISTRIBUTION COMPANIES AND GAS COMPANIES IN RESTORING SERVICE FOLLOWING STORM SANDY (2013), *available at* http://www.dpuc.state.ct.us/FINALDEC.NSF/0d1e102026cb64d98525644800691cfe/0072d9132451b44e85257bce00685d3a?OpenDocument&Highlight=0,storm. Connecticut's public utility commission, called the Public Utilities Regulatory Authority, evaluated the companies' storm preparations, emergency planning, communications, storm restoration, and response and concluded that "these companies performed in a generally acceptable manner in preparing for and responding to the storm. The Public Utilities Regulatory Authority finds that improvements are necessary in certain areas, and orders these companies to make such improvements to their policies, practices and procedures . . . ." *Id.* at 1.

312. REPORT OF THE ENQUIRY COMMITTEE, *supra* note 9.

Several of the recommendations made by the Report are remarkably similar to those expressed by the CATF and SIRTF Reports (regarding the handling of Severe Events). Most of the major recommendations direct attention to the readiness to handle post-event recovery and restoration efforts. The NERC Task Force focused on "graceful degradation" of operations into "islands" of electric power and the need to stabilize them throughout the period of recovery and restoration. The India Grid Disturbance Report recommended:

> There is need to plan islanding schemes to ensure supply to essential services and faster recovery in case of grid disruptions.
>
> . . . .
>
> . . . [I]t was agreed that criteria for formation of islands should not be the geographical or electrical size but reliability of load-generation balance in the islands. . . .
>
> . . . .
>
> As far as possible, major essential loads such as hospitals etc should be incorporated in the islands. However, if this was not possible due to some reasons, efforts would be made to extend supply from these islands to essential loads on priority basis.
>
> . . . .
>
> Efforts should be made to design islanding scheme based on frequency sensing relays so that in case of imminent grid failure, electrical islands can be formed. These electrical islands can not only help in maintaining supply to essential services but would also help in faster restoration of grid.[313]

2. Counsel's Recommendations

We think the focus of everyone within the area affected by a "high-impact, low-frequency" event tends to be on resilience and recovery—how well prepared, organized, and effective did the critical infrastructure companies appear during their efforts (over many weeks) to restore electric power and telecommunications

313. *Id.* at ix, 40, 41, 67. The Report also included a set of recommendations for "islanding of Delhi metro and Indian Railways" to spare them the worst effects of grid disturbances. *Id.* at 41.

after Hurricane Sandy?[314] We think it is reasonable to infer that similar standards and judgments will be applied to owners and operators of BPS and other critical infrastructure in the weeks, months, and possibly years following a Severe Event caused by a coordinated and adaptive cyber attack.

The more prolonged the attacks, the more adaptive they prove to be, and the more sophisticated their exploits, the more we think it probable that the public will not blame or judge critical infrastructure companies for being "knocked out"—provided that such companies and the federal government disclose such facts to the public (which remains an open issue and one that boards and management will also need to review). But the withholding of judgment for succumbing to a Severe Event will only increase the scrutiny and severity of judgment that the public, the regulators, and the media give to owners and operators of BPS and other critical infrastructure during the New Normal period. To the extent that such companies appear to have prepared to manage and carry out "graceful degradation" of operations and services, to handle the long-term restoration, and to maintain and repair the necessary "islanding" of electric power, telecommunications, and other vital services, such companies will be judged favorably. If they prove ill prepared and lacking in resourcefulness to handle the prolonged crisis, then their reputational damage will probably be extensive, and possibly irreparable. The public, the media, and the government may point to all the warnings such companies received—and particularly the recommendations contained in the CATF and SIRTF Reports (which will probably get long overdue attention after a Severe Event)—and claim "after such knowledge, what forgiveness?"[315]

314. After Hurricane Sandy, electric utilities in New York, New Jersey, and Connecticut have been participating in regulatory proceedings that investigated the adequacy of storm response (*see, e.g.*, PUB. UTIL. REGULATORY AUTH., *supra* note 311) and to request extraordinary rate recovery in advance to allow some of these companies to make investments to "harden" or make more resilient their electric transmission and distribution grid infrastructure. These investments typically mean relocating substations away from coastal areas, building storm walls around critical infrastructure, or burying power lines to avoid tree falls during storms. *See id.* at 54–55.

315. T.S. ELIOT, *Poems 1920, Gerontion*, *in* THE COMPLETE POEMS & PLAYS OF T.S. ELIOT 38 (1969).

VIII. CONCLUSION: COUNSEL'S QUALIFYING RECOMMENDATIONS—TECHNOLOGY'S SINISTER SURPRISES

A. Closing Caveats—the Murky Challenges

We noted early in this article that a drawback of the White House's 2013 initiatives has been that the EO and its announcement in the President's State of the Union address made the cybersecurity threat and requisite response far too neat, clean, clear, and straight-forward.[316] We return to that theme in this conclusion because counsel's recommendations, when organized under a logical sequence of questions and answers, can similarly distort and make too neat and clean the challenges facing owners and operators of critical infrastructure, which must be seen for what they are and will probably continue to be for the foreseeable future—complicated, messy, murky, and disorienting. One purpose of this discussion has been to make those features more apparent than they have tended to be in the White House initiatives. Another purpose has been to give boards, management, and counsel a cold, hard, realistic view of the challenges presented by cyber threats that target critical infrastructure. To ensure that this discussion closes with an appreciation of the magnitude and messiness of the challenges to critical infrastructure's operational resilience (especially to the resilience of the BPS), we will discuss in this conclusion some of the most recent disclosures of vulnerabilities in the BPS, the ease with which adversaries could exploit them, and the growing sophistication of the tools and cyber weaponry that adversaries can use to target, disrupt, and damage the BPS.

Counsel will need to consider bringing these and other emerging developments to the attention of a BPS company's board and management. The goal is to ensure the sufficiency of plans and preparations the company might be making in anticipation of coordinated cyber attacks designed to sabotage operations, Severe Events, post-attack graceful degradation, "islanding" of electric power, and New Normal periods of prolonged reduced operations and restoration of services. Counsel's focus will need to be on helping guide the BPS company (or other critical infrastructure

316. *See supra* Part IV.G.

enterprise) to achieve *enhanced readiness* for the worst-case consequences from a cyber attack on company operations.

B. Recently Disclosed Vulnerabilities

We will review two recently disclosed vulnerabilities related to operation of the BPS or to operations that are interdependent with the BPS: (i) vulnerabilities that continue to be introduced into the BPS system by deployment of "smart grid" technologies; and (ii) vulnerabilities discovered in the software used in BPS SCADA systems.

1. Deployment of "Smart Grid" Technologies Proliferate Vulnerabilities in the BPS

The crux of each "smart grid" technology deployed in the BPS is that it seeks to create a *two-way communications link or channel* that would, among other things, provide home customers real-time information about the fluctuating costs of electricity so that they could schedule power-intensive activities (such as operating a clothes dryer or dish washer) during off-peak (i.e., cheaper) time periods. As summarized by the DoE, the characteristics of a "smart grid" by the year 2030 will be (in its overly optimistic view):

> [A] fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between. Its distributed intelligence, coupled with broadband communications and automated control systems, enables real-time market transactions and seamless interfaces among people, buildings, industrial plants, generation facilities, and the electric network.[317]

The key phrase in this description is "two-way flow" of communications. Each two-way flow of communications offers a potential vulnerability or portal into a network that cyber adversaries can exploit. As explained in a 2011 Congressional Research Service report:

317. OFFICE OF ELEC. TRANSMISSION & DISTRIB., U.S. DEP'T OF ENERGY, "GRID 2030": A NATIONAL VISION FOR ELECTRICITY'S SECOND 100 YEARS 17 (2003), *available at* http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Electric_Vision_Document.pdf.

> Grid devices capable of two-way communications are considered to be potential points of unauthorized system access, and can represent a potential cybersecurity vulnerability. . . . Smart meters are another example of new applications in which the security of data has been mentioned as a concern.[318]

The U.S. Government Accountability Office (GAO), in 2011, expressed similar concerns but viewed them in a broader context of vulnerabilities:

> The smart grid vision and its increased reliance on IT systems and networks expose the electric grid to potential and known cybersecurity vulnerabilities associated with using such systems, which in turn increase the risk to the smooth and reliable operation of the electricity grid. . . . [T]hese potential vulnerabilities include:
>
> - increasing the use of systems and networks increases the number of entry points and paths that can be exploited by potential adversaries and other unauthorized users;
> - interconnecting systems and networks can allow adversaries wider access and the ability to spread malicious activity . . . .
>
> . . . .
>
> In addition, we reported in 2007 that certain smart systems—commonly referred to as control systems—used in industrial settings such as electric generation have cybersecurity vulnerabilities that, if exploited, could result in serious damages and disruption. . . . Moreover, in 2008, the Central Intelligence Agency reported that malicious activities against IT systems and networks have caused disruption of electric power capabilities in multiple regions overseas, including a case that resulted in a multicity power outage.[319]

The release of these government reports highlighted the vulnerabilities that "smart grid" technologies contain and will, therefore, embed when deployed within the BPS. Despite the growing possibility that such vulnerabilities could provide attack

318. RICHARD J. CAMPBELL, CONG. RESEARCH SERV., THE SMART GRID AND CYBERSECURITY—REGULATORY POLICY AND ISSUES 7 (2011), *available at* http://www.fas.org/sgp/crs/misc/R41886.pdf.

319. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 226, at 10–11 (citations omitted).

vectors for adversaries seeking to launch kinetic cyber attacks against a BPS company's operations, owners and operators of BPS companies appear to be focusing solely on the high (and overly optimistic) promised benefits of creating the "smart grid." We think they should instead give early and enhanced attention to discovering and correcting the technology's high-risk vulnerabilities. As noted by the Center for Strategic and International Studies Report:

> Despite these vulnerabilities, many power companies are doubling down on the danger; they are implementing "smart grid" technologies that give their IT systems more control over the delivery of power to individual customers—or even to individual appliances in customers' homes. . . . But security is not a priority for smart grid designers; according to Woolsey, who two years ago chaired a group that published a report for the Department of Defense on grid vulnerabilities. "Ninety to ninety-five percent of the people working on the smart grid are not concerned about security and only see it as a last box they have to check."[320]

As BPS companies pursue deployments of "smart grid" and involve third-parties to design, develop, and install the devices, it will be increasingly important for boards and management to be assured that such "progress" is not progressively making the company's operations more susceptible to advanced persistent attacks by creating vulnerabilities adversaries could exploit. Unfortunately, to date, that seems to be the risk—and there appears to be little effort to avert that outcome. Thus in GAO testimony to Congress in 2012:

> Security features had not been consistently built into smart grid devices. . . . [T]hus increasing their vulnerability to attack. Without securely designed smart grid systems, utilities may not be able to detect and analyze attacks, increasing the risk that attacks would succeed and utilities would be unable to prevent them from recurring.[321]

Boards and management may not be comfortable asking if the promise of the "smart grid" is going to be outweighed by the

320. BAKER ET AL., *supra* note 31, at 1.

321. WILSHUSEN & TRIMBLE, *supra* note 6, at 13.

vulnerabilities and risks it introduces into a BPS company's operational systems. However, such questions become more compelling each time one considers them in the context of the threats identified by the CATF and SIRTF Reports and the growing possibility of Severe Events. What would be particularly helpful in this regard would be if NERC would have a task force analyze and assess the probable consequences of a Severe Event from a cyber attack occurring in a BPS company that had extensively deployed "smart grid" technology and was therefore that much more dependent on complex and hard-to-balance systems.

2. Vulnerabilities Recently Disclosed in the North American BPS

As mentioned above, approximately a month after the President issued the EO, two engineers detected defects in a communications protocol, DNP_3, which BPS companies have extensively installed in SCADA systems to monitor distant power stations from an air-gapped control center.[322] When they tested DNP_3 made by Triangle MicroWorks, the software "broke instantly."[323] They tested DNP_3 made by sixteen other vendors and obtained the same destructive results.[324] Although they reported their findings within a week to DHS's ICS-CERT, it took four months for ICS-CERT to start to issue advisory alerts to BPS owners and operators.[325] During that time, the engineers found such defects in the software made by another nine vendors. At the same time, the first vendor whose wares they tested, Triangle MicroWorks, had developed an update that purportedly mitigated the vulnerability.[326] The risks these defects create in the BPS were explained in a recent *New York Times* article:

> [One of the engineers] found that he could actually infiltrate a power station's control center from afar. An attacker could use that capability to insert malware to take over the system, and like Stuxnet, the computer worm that took out 20 percent of Iran's centrifuges, inflict actual physical harm.
>
> . . . .

322. *See* Perlroth, *supra* note 73.
323. *Id.*
324. *Id.*
325. *Id.*
326. *Id.*

> What makes the vulnerabilities particularly troubling, experts say, is that traditional firewalls are ill-equipped to stop them. When the master crashes it can no longer monitor or control any and all of the substations . . . . There is no way to stop this with a firewall and other perimeter security device today. You have to let DNP_3 responses through.[327]

There are two such defects. Both kinds "incorrectly validate[] input" and enable an attacker to "cause the software to go into an infinite loop . . . causing the process to crash. The system must be restarted manually to clear the condition."[328]

The ICS-CERT advisory recommended that BPS companies install the update and take additional precautions.[329] In addition to that late August 2013 advisory, ICS-CERT issued, on October 21, 2013, a similar advisory concerning DNP_3 made by a different vendor.[330] The advisory recommended the same precautions—plus an additional mitigation: "Block DNP_3 traffic from traversing onto business or corporate networks through the use of an IPS or firewall with DPN3-specific rule sets."[331]

In substance, these advisories caution that BPS companies may have such software—and the embedded defects—resident on their control systems. This makes their operations vulnerable to a cyber adversary seeking to take over the company's operational system. If successful, that exploit could provide a good foundation for an attack directly against the company's equipment and operations. It is unclear whether the EO's direction for creation of the Framework will address such vulnerabilities. Equally important, the existence of these vulnerabilities evidences the enhanced probability that a cyber adversary could launch an attack against a BPS company that could cause a Severe Event. Counsel will want to bring these and similar advisories to the attention of boards and management, not for discussion of the technical details, but to ensure that the technical staff of the company will promptly install the corrective updates or "patches." Such vulnerabilities

327. *Id.* (internal quotation marks omitted).

328. Advisory, ICS-CERT, *supra* note 75.

329. *Id.*

330. Advisory, ICS-CERT, Alstom e-Terracontrol DNP3 Master Improper Input Validation (Update A) (rev. Dec. 17, 2013), http://ics-cert.us-cert.gov/advisories/ICSA-13-282-01A.

331. *Id.*

demonstrate the extent to which the cybersecurity posture of a BPS company is becoming increasingly messy and murky. Furthermore, the discovery of these vulnerabilities, and the reactive nature of ICS-CERT's response, suggests strongly that prudent critical infrastructure owners and operators cannot wait for the next ICS-CERT alert. BPS companies need to be ever vigilant and proactively testing systems for vulnerabilities.

3. Closing Observations

We have argued throughout this article that it would be prudent for counsel to advise owners and operators of critical infrastructure to give serious consideration to placing their highest and most urgent priority attention on managing Severe Events and the consequences that arise throughout the following New Normal period.[332] In giving such advice, however, counsel might also find it prudent to recommend that owners and operators of BPS companies treat the threats as serious and potentially imminent, because once they prove to be, it will be too late to make the necessary preparations.

Lastly, counsel may also find it wise to recommend that as owners and operators of BPS companies prepare to manage "electric islands" and archipelagos of isolated services, with the requisite stabilizing use of scheduled "load shedding" and rolling outages, they should be working closely with other critical infrastructure as much as possible rather than in isolation as if they could spare themselves without making sure that they protected others. This recommendation is based on the assumption that progress in improving cyber defenses continues to fall ever further behind the progress being made in improving cyber weaponry and attack sophistication. As a result, attacks can be designed to be far *better coordinated* than the defenses and responses to an attack once it is detected. Moreover, many intrusions are so stealthy that they remain undetected for months. And even then, their mode of operations and objectives may elude the operators and owners of

332. We strongly recommend that BPS operators and their counsel carefully review the SIRTF and CATF Reports, as both documents are unmatched in their extensive detail and the work product resulting from extensive industry collaboration on these task forces proves extremely useful. *See* CATF REPORT, *supra* note 13; SIRTF REPORT, *supra* note 13.

the targeted companies.[333] As a DHS paper noted, commenting on the imbalance between the formal modes of sophisticated (advanced persistent threat) attacks and the ad hoc defenses currently relied upon for protection: "Cyber defense today is founded on *ad hoc*, manual processes; yet cyber attacks often follow a well known, systematic escalation path beginning with reconnaissance activities and extending to gaining entry, establishing persistence, setting up external communications pathways, and conducting attack operations."[334]

In preparing for such conversations in which some added perspective is always useful to avoid an overly technical and complex approach, counsel might even find it worth considering the need for BPS boards and management to take care to include consideration of the interconnectedness of the BPS company's operations with those of other critical infrastructure—and the need for readiness should a Severe Event occur as a result of a coordinated cyber attack against the company.[335] We offer in

333. The stealth and delay in detection partially explain why "hackers are able to sell previously unknown software vulnerabilities, known as 'zero days' because of the time between discovery and the first attack, for six-figure sums . . . ." Chris Bryant, *Rethink on 'Zero-Day' Attacks Raises Cyber Hackles*, FIN. TIMES (London), January 15, 2014, at 4. Moreover, the National Security Agency appears to have gone a step further because it reportedly "has implanted software in nearly 100,000 computers around the world that allows the United States to conduct surveillance on those machines and can also create a digital high-way for launching cyberattacks." David E. Sanger & Thom Shanker, *N.S.A. Devises Radio Pathway into Computers—Reaching Targets Cut Off from Internet*, N.Y. TIMES, Jan. 15, 2014, at A1, *available at* 2014 WLNR 1172743. It has done this even to computers not connected to the Internet. *Id.*

> The technology, which the agency has used since at least 2008, relies on a covert channel of radio waves that can be transmitted from tiny circuit boards and USB cards inserted surreptitiously into the computers. In some cases, they are sent to a briefcase-size relay station that intelligence agencies can set up miles away from the target.

Id.

334. ENABLING DISTRIBUTED SECURITY IN CYBERSPACE 6 (2011), *available at* http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

335. In this regard, the SIRTF Report recommends anticipating the needs of those who depend on the BPS company owners and operators to keep them apprised of the status throughout the New Normal period:

> Throughout the New Normal period, people will need to understand how restoration is proceeding so they can make their own decisions to

closing expressions of those themes in passages from two writers. First, consider the lines from John Donne's *Devotions Upon Emergent Occasions, Meditation XVII*, where he memorably wrote a caution for his congregants that owners and operators of BPS companies might find it in their best interest to heed:

> No man is an *Iland*, intire of it selfe; every man is a peece of the *Continent*, a part of the *maine*; if a *Clod* bee washed away by the *Sea*, *Europe* is the lesse, as well as if a *Promontorie* were, as well as if a *Mannor* of thy *friends* or of *thine owne* were; any mans *death* diminishes *me*, because I am involved in *Mankinde*; And therefore never send to know for whom the *bell* tolls; It tolls for *thee*.[336]

Second, consider the observations of Shakespeare's Hamlet who broods about the inevitable arrival of certain momentous events and the need, when such times come, to be ready: "There is special providence in the fall of a sparrow. If it be now, 'tis not to come—if it be not to come, it will be now—if it be not now, yet it will come—the readiness is all."[337]

Boards and management of critical infrastructure companies know well the need for "readiness." However, it will fall to their counsel to bring to their attention that, amidst the multiplicity of identified cyber threats and applicable standards and recommendations, the best course continues to be to focus on the worst-case scenario of Severe Events and the prolonged New Normal periods of degraded operations. A company's handling of those will remain its most challenging test and the one by which its customers, regulators, and other critical infrastructure owners and operators will ultimately judge it to have acted responsibly or otherwise. In this era of new corporate cyber responsibilities, we

> care for themselves, their family, and their community. If there is limited information available from media outlets, entities could consider posting important information (e.g., rotating blackout schedules) at government offices such as police stations or post offices and at locations where people will congregate (e.g., food and water delivery points).

SIRTF REPORT, *supra* note 13, at 44.

336. John Donne, *Devotions Upon Emergent Occasions, Meditation XVII, in* THE COMPLETE POETRY AND SELECTED PROSE OF JOHN DONNE 445, 446 (Charles M. Coffin ed., 2001) (emphasis in original).

337. WILLIAM SHAKESPEARE, THE TRAGEDY OF HAMLET, PRINCE OF DENMARK act 5, sc. 2.

believe that focus will best protect a critical infrastructure company and help assure a board and management that they are fulfilling their fiduciary duties for the enterprise and its cybersecurity.