

The Honorable Franklin D. Kramer is a national security and international affairs expert. Mr. Kramer has been a senior political appointee in two administrations, including as Assistant Secretary of Defense for International Security Affairs for President Clinton, Secretary Perry and Secretary Cohen; and, previously, as Principal Deputy Assistant Secretary of Defense for International Security Affairs. At the Department of Defense, Mr. Kramer was in charge of the formulation and implementation of international defense and political-military policy, with worldwide responsibilities including NATO, the Middle East, Asia, Africa and Latin America.

In the non-profit world, Mr. Kramer is vice chairman of the Atlantic Council board of directors; a Senior Fellow at CNA; a capstone professor at the Elliott School of International Affairs; George Washington University; has been chairman of the board of the World Affairs Council of Washington, DC and is currently chairman of the International Education Committee; and has been a distinguished research fellow at the Center for Technology and National Security Policy of the National Defense University. In the private sector, Mr. Kramer is a director and consultant and has been a partner at the law firm of Shea & Gardner.

Among his recent activities, Kramer is the principal editor and has written several chapters for the book "Cyberpower and National Security," and is the author of "Cyber Security: An Integrated Governmental Strategy for Progress." He is likewise the principal editor, and co-author of the policy chapter, of the book "Civil Power in Irregular Conflict," and the author of the forthcoming "Irregular Conflict and the Wicked Problem Dilemma: Strategies of Imperfection." He is the co-author and co-project director of "Transatlantic Cooperation for Sustainable Energy Security" and of "Central Europe and the Geopolitics of Energy." At George Washington University, he teaches a course on "The Department of Defense and Winning Modern War."

He has written numerous articles on international affairs including "NATO Initiatives for an Era of Global Competition," "Recasting the Euro-Atlantic Partnership," "Cyber Influence and International Security," "Making Peace Stick in Lebanon," "Taiwan: Avoiding a Train Wreck," and military power and "Tools to Win the Peace." He has chaired numerous task forces and conferences, including on post-conflict stability operations, on overseas basing, on China and the world economy, and on China-Taiwan-U.S. relations. He has given speeches on cyber security and cyber conflict, on energy and security, on the role of great powers in a globalizing world, on the future of NATO and the Partnership for Peace; and on the U.S.-India defense relationship. He has testified frequently, including since leaving the government on topics ranging from Chinese military power to strategic communications to cyberpower.

Mr. Kramer graduated magna cum laude with a JD from Harvard Law School and cum laude with a bachelor's degree from Yale University.

Statement of Franklin D. Kramer  
before the  
House Energy and Commerce Committee  
Subcommittee on Energy and Power  
May 31, 2011

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify on the subject of cyber security and the electric grid. I am appearing today solely in my individual capacity, and my testimony is only my own.

To summarize, my key points are: the need for mandatory government-generated standards since the current approach is insufficient; the importance of being able to generate resilience of the electric grid in the face of attack; the need to use all the capabilities of the federal government to protect the grid, including those of the Department of Defense and the intelligence community working in conjunction with the agency responsible for electric grid security and with the private sector; the requirements of scale and resources; and the need to include the distribution system under an effective cyber security approach for the electric grid.

The testimony which follows is divided into three parts:

- the threats to and vulnerabilities of the electric grid, and the national security implications potentially resulting from an attack on the grid;
- the requirements of an effective cyber security approach for the electric grid;
- and
- the extent to which the GRID Act and other proposed legislation meet or could be improved to meet those requirements.

1. Threats, Vulnerabilities and National Security Implications. The electric grid's vulnerability has been well-documented on numerous occasions, including hearings before this Committee, statements by the President of the United States, and numerous governmental and other studies. The electric grid has become substantially dependent on cyber capabilities over the past 15 years, and the well-known attacks on Google, RSA, and Comodo—three very highly capable information technology companies--as well as the STUXNET and WikiLeaks incidents, underscore the vulnerability of cyber infrastructures—vulnerabilities which are all shared by the electric grid.

From a technological point of view, these vulnerabilities raise issues of remote attack (with multiple vectors); close-in attack; insider attack; and possibly in the broader Iranian nuclear context, supply chain attack. All involve critical technical vulnerabilities and exploits.

From a policy point of view, they raise the issues of protection, prevention, and resilience—and the questions of scale, resources, and governance necessary to accomplish those tasks.

The importance of recognizing this vulnerability cannot be overstated. The vulnerabilities exist despite the existence of cyber security standards for the electric grid which have been promulgated under Section 215 of the Federal Power Act.

The North American Electric Reliability Council’s High Impact, Low Frequency study issued in June 2010 stated “the bulk power system remains an attractive target for acts of both physical and cyber terrorism,” and further concluded:

“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. . . . [A] coordinated attack would involve an intelligent adversary with the capability to quickly bring the system outside the protection provided by current planning and operating practices. An outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods.”<sup>1</sup>

The impact would be very significant, both from a national security and an economic perspective. As I have noted in prior writing: “There is an important additional reason why the grid deserves high level attention: the DOD cannot function without electricity. While there is considerable focus in the DOD at this time on that vulnerability, and many efforts toward off-grid power solutions, very significant vulnerability currently exists and will continue to exist for a long time. Further, even if the DOD made its own facilities relatively immune to grid disruption, the Pentagon depends heavily on other civilian

---

<sup>1</sup> NERC, High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, at p. 26.

infrastructures that themselves rely on electricity, the most obvious being telecommunications, but also all elements of transportation and logistics.”<sup>2</sup>

What is true of the Department of Defense is true of virtually all governmental, private sector and individual functions in the United States. As an advanced technological nation, we run on electricity.

During the past year, we have had even further confirmation of the problem of the grid’s vulnerability, as demonstrated by the STUXNET attacks.

STUXNET—while not grid-directed, showed the vulnerability of control machines—which are the very type of machines upon which the grid depends for effective operation. STUXNET has been publicly analyzed in numerous places, and the Committee will be fully familiar with its implications.

STUXNET shows also that not only are the offense and defense at play in the cyber arena—but if one accepts numerous public accounts (such as set forth in the New York Times and many other places) that the offense is well ahead of the defense.

Finally, one important ongoing change for the grid is the expected emergence of the smart grid. The smart grid has multiple aspects, but a key element will be the connectivity between the consumer, supplied by the distribution system, and the generation/transmission portions of the grid. Such connectivity means that the distribution system could be a key vector for a national security attack on the grid. That is a newly significant issue, and one which deserves this Committee’s consideration.

In sum, the vulnerability of the electric grid is a critical national security problem. Failure to resolve it could have devastating national security and economic consequences.

2. Requirements of Effective Cyber Security for the Electric Grid. Effective cyber security for the electric grid will have three key elements, including A) key cyber security capabilities, B) appropriate cyber security governance directed to the roles and responsibilities of the federal government and the private sector, and C) continuing efforts on research and development to generate currently needed capabilities and meet future threats.

A. Capabilities. The requirements of cyber security for the grid include:

---

<sup>2</sup> Kramer, Cyber Security: An Integrated Governmental Strategy for Progress, at p. 8 (2010).

--First, the problem of protecting interlocking multiple, including some very large, enterprises—there are some 3200 power generation companies in the North American grid. Thus, the problems of scale and the resources necessary to act are critical to consider.

--Second, the issue of appropriate technologies and processes, including the necessity of trained personnel. There currently is no agreed architectural approach that companies can use to provide adequate cyber security—that is why current vulnerabilities exist, and why existing standards are not sufficient. And there are insufficient trained cyber security experts.

--Third, the need to be able to operate despite attack. All believe that under current conditions, cyber offense beats cyber defense, so the question is, expecting to have cyber defenses penetrated, how to keep the appropriate elements of the grid effectively operating. The most important requirement of cyber security for the electric grid will be its resilience under attack.

The cyber security requirements challenge, therefore, is to develop:

- 1) an overall approach including technologies and processes,
- 2) courses of action that, based on the technologies and processes, provide resilience, and
- 3) the people capable of doing this.

It is also important to recognize that successful cyber security likely will involve a strategic framework that goes beyond defense and resilience. In protecting Department of Defense networks, the DOD is also focused not only on passive defense, but also on “active defense” and “offensive” cyber. “Active defense” means using sensors and capabilities at the perimeter of the DOD enterprise to affect the attacker. “Offense” means using cyber as one would any other DOD capability—kinetic or electronic warfare, for example. It certainly is not the case that any private enterprise without government involvement could or should undertake active defense or offensive action, as the DOD has prepared for (although, of course, private entities can protect their own networks, technology and information with appropriate measures<sup>3</sup>). However, if DOD networks require this type protection, it would appear that such protection would be important to the electric grid were it under attack.

---

<sup>3</sup> One important legislative question is to what extent and under what circumstances, including possibly government authorization, should Internet Service Providers undertake protection from the network for their customers.

Accordingly, it would seem appropriate for the DOD with the right legislative authority and under Presidential guidance to help protect electric grid networks. To paraphrase the substance of what one electric power company official said to me (and this is a paraphrase), “I can understand why my company should be able to protect itself against cyber criminals, but why should I be expected to succeed against a major nation state cyber attack? Isn’t that what the government is supposed to do?” That seems to me to be a critical point—a major nation state attack (or a major attack by a terrorist organization) will be different in character and consequence from an attack by criminals against an enterprise. Accordingly, given the consequences of such an attack, I believe legislation should clearly authorize the DOD and the intelligence community, under appropriate guidelines and working with the agency responsible for electric grid cyber protection and with the private sector, to take both anticipatory and responsive steps to protect the grid and to ensure its resilience if it were under such attack.

B. Governance. Inasmuch as the vulnerability of the electric grid presents a national security vulnerability of high consequence, there is, as this Committee’s proposed Grid Act indicates, an extremely strong case for new legislation and regulation that would set forth a fully integrated framework to deal with this problem. The current legislative and regulatory governance approach, though it has accomplished some things, has not been sufficiently effective. Just as strong safety requirements for cars and environmental requirements limiting water and air pollution have greatly improved the national posture, legislation and regulation that created an effective requirement for much stronger cyber security for critical infrastructure like the electric grid would meet an important national need. While there is a compelling need for new legislation and regulation, three important considerations need to be taken into account.

First, since the grid is very largely in private hands, but the government has critical capabilities, there needs to be an effective public-private working relationship. However, the current Section 215 process has not provided the degree of cyber security that is adequate. Accordingly, rather than an approach that relies on industry to generate cyber security standards, the federal government should have the responsibility to do so. Generally, the government should act after consultation with industry. However, if there is a significant threat that prompt government action would mitigate, government action should be authorized. That approach is different from the imminent threat standard in the proposed Grid Act. Enhancing cyber security often will be best

accomplished by taking steps well in advance of an imminent threat—for example, in response to reconnaissance by an adversary or otherwise early in the threat cycle, and it may be invaluable not to have to wait for a full-blown regulatory process.

Second, enhancing cyber security may require costs of some consequence to the industry. Legislation should take account of that fact, and that the industry operates under regulatory constraints. Focus on cost recovery would be especially appropriate if industry were required to act where prompt action was required based on a federal decision. But it should also be true when requirements are imposed more generally for national security and national economic purposes. Since cyber security is so critical to the nation, the industry should be able to recover its costs—which could come about through direct or indirect cost recovery from the federal government or through a rate base approach.

Third, the cyber sector has had a very quickly changing nature. Cyber looks very different today than it looked only ten years ago, and there are good reasons to believe that it will significantly change again in ten years. Any regulatory scheme that is not flexible enough to take account of such changes is likely to be far less effective than necessary.

C. Research and Development. As the Google matter and other well-known intrusions show, even very capable companies with extensively deployed cyber security measures are vulnerable. Current capabilities can only go so far. It is generally agreed that an advanced attacker will be able to negate currently available defenses.

The fundamental question that this issue raises, therefore, is whether an enhanced cyber security capability can be created. Or, to put it another way, how valuable would a significant R&D program be? And most specifically, in the context of this hearing, what does that mean for the electric grid? Could, for example, the grid's network nature and topology be taken advantage of to provide resilience in a way that might not be available to a more point type target such as an enterprise or cloud or individual? If it would seem to be valuable, how should such R&D be undertaken, including what should the division of labor be between government and the private sector (including how the government should appropriately leverage private investment)?

There are, of course, many existing R&D efforts. The Department of Energy, particularly through the DOE laboratories, has undertaken excellent research focused on the grid. Many cyber security issues overlap in multiple arenas beyond the grid, and important efforts exist under DOD and intelligence community auspices, including efforts by the Defense Advanced Research Projects Agency (DARPA). Others are at the Department of Homeland Security, which has developed a cyber security R&D program, and at the National Academy of Sciences. There are also substantial resources from the private sector, some in response to the government programs and some independent R&D.

A much enhanced R&D program, including increased efforts focused on the electric grid, nonetheless would be highly valuable to improve cyber security. Such a program could likely profitably be divided among the government (which could do more pure research than in the private sector, could focus on particular types of applications and could help guide private research) and the private and academic sectors (which could benefit from increased government support, but which also will undertake research on their own in order to meet market demands). The key considerations are to have an integrated view of federal cyber security R&D and to ensure that appropriate amounts are being spent on developing particular solutions. Substantively, such an R&D program should have three parts:

- The first would focus on protection – can advanced techniques such as dynamic addressing and moving targets; and segmentation/tailored trustworthy spaces be developed to create much enhanced cyber security.
- The second would assume, as seems entirely likely, that security will not be perfect and will therefore focus on resilience – how to operate a system effectively even though security has been breached. What, for example, would be necessary to implement gold standard integrity for data, software and hardware; how might redundancy or diversity be used to support resilience?
- A third key element would be to develop a systematic approach to measuring security. One element of this would be to greatly enhance the area of modeling and simulations to test the results of both attacks and defenses.

In addition to specific R&D approaches, one important, long-term approach to enhanced R&D would be to greatly expand education and training for cyber

professionals. A significantly increased governmental education/ scholarship program would be very valuable.

3. The GRID Act and Other Proposed Legislation. As the foregoing suggests, the proposed Grid Act and other currently proposed legislation would be substantial improvements on the existing legislation. Focusing on the Grid Act and without reviewing each element of the other legislative proposals, the following recommendations would significantly improve suggested legislation.

A) Legislation should give the government mandatory regulatory authority over the grid, and should eliminate the approach whereby the government (now FERC) only has authority to review reliability standards recommended by the North American Electric Reliability Council. That approach has not provided adequate security and is far too slow in a context of a highly dynamic and dangerous threat environment.

B) Reliability standards should include authorization to require specific technological approaches and processes, as well as personnel requirements. Specific focus should be put on the requirements of resilience since the expectation must be of a breakdown in security—and the need will exist to maintain an adequate level of electric power operations even when the grid is under attack. That may mean that the standards will be significantly higher and that there could be significantly greater requirements for parts of the grid than for others (and advanced capabilities may be particularly important for these parts of the grid). Performance standards are a desirable longer term goal, but until greater R&D has been accomplished, performance standards are unlikely to be feasible for the most part.

C) The Department of Defense and the intelligence community should be legislatively authorized to work with the agency responsible for electric grid security and with the private sector to provide under appropriate guidance anticipatory and responsive actions (to achieve protection, prevention and resilience).

D) The interconnectivity of the grid and its very large scale means that getting effective cyber security capabilities out to the full grid and the resources necessary to do so are highly important. An evaluation/certification process probably will be valuable, although, to be effective, reliability standards will have to be issued against which evaluation/certification can be undertaken. Additionally, since companies whose rates are often regulated are being asked

to work with the federal government to help resolve a national security problem, there should be a mechanism for costs to be recovered. That could be directly or indirectly with the federal government or under a rate base approach.

E) The emergence of the smart grid means that the distribution system can be an important vector for a cyber attack. Cyber security legislation and regulation therefore needs to include the distribution system if effective electric grid security is to be achieved.

F) An expanded R&D program should be undertaken in order that advanced capabilities to meet the dynamic and changing threat can be achieved.

Finally, any efforts by this Committee should, of course, be coordinated with the other committees proposing legislation, both in the House and in the Senate.

\* \* \* \* \*

I thank you very much for the opportunity to testify, and look forward to your questions.