TESTIMONY OF DR. MICHAEL J. FRANKEL

HOUSE HOMELAND SECURITY COMMITTEE HEARING

SUB-COMMITTEE ON CYBER SECURITY, INFRASTRUCTURE PROTECTION,

AND SECURITY TECHNOLOGIES, HOUSE CANNON OFFICE BUILDING,

ROOM 311, MAY 8, 2014

Mr. Chairman and Honorable Members of the Committee, thank you for the opportunity to testify today about an important but relatively neglected vulnerability that affects the resilience of all of our nation's critical infrastructures. My name is Mike Frankel. I'm a theoretical physicist by trade and presently a member of the senior scientific staff at Penn State University's Applied Research Laboratory. I've spent a career in government service developing technical and scientific expertise on the effects of nuclear weapons, managing WMD programs, and performing scientific research in a variety of national security positions with the Navy, the old Defense Nuclear Agency, and the Office of the Secretary of Defense. I appear before you today pursuant my service as the Executive Director of the EMP Commission during its entire span of activity, commencing with authorization if the Floyd D. Spence National Defense Authorization Act of 2001 and culminating with delivery of its final, classified, assessment to the Congress in 2009 The conclusions of the Commission were documented in a series of five volumes, three of them classified, and in particular the Commission's perspectives related to infrastructure protection were documented in an unclassified volume *"Critical National Infrastructures",* released in November of 2008. What I'd like to do is expand on some of the Commission's conclusions in light of recent developments since submitting our final report. I should also like to emphasize a new topic that was not referenced in that final report, and that is the nexus between the cyber security threat and EMP.

One of the major insights of the EMP Commission was to highlight the unique danger to the electric grid caused by simultaneous failures induced by the large number of components that fall within an EMP's damaging footprint on the ground. As first reported in the journal Foreign Affairs and picked up a month later by the Wall Street Journal, on the night of April 16, 2013, a locked PG&E substation was infiltrated and a number of high voltage transformers attacked by still unidentified individuals firing rifles. Damaged transformers went off line but the SCADA controls automatically re-routed the electrical distribution along alternate paths. In this case, standard engineering practice

which designs around the possibility of single point failure, kicked in just as it should. and little effect was noticed by the general population. However, it took nearly a full month to repair the damaged transformers and return them to service. An important analytic contribution of the Commission was to highlight the possibility of highly multiple numbers of component failures, as might be expected within the wide area encompassed by an EMP event footprint. No one designed against such a possibility and it was the Commission's conclusion, based on its own analyses and on a close collaboration with power industry engineers, that such a scenario would inevitably lead to very wide spread, and very long term collapse of the nation's electric grid, with potentially devastating economic and ultimately physical and health consequences. The PG&E incident should remind us that the Commission's analytic insight extends far beyond EMP. While in this case only a single substation was attacked, had there been a coordinated physical attack against many simultaneous targets, or for that matter by localized EMP sources such as readily available HPM/RF sources, it seems inevitable that electric service to much larger fraction of the population would have been compromised and for an indefinitely prolonged period. And of course, the same result could be achieved by simultaneous cyber-attack, with much reduced physical exposure by the perpetrators. So there's a real vulnerability there that needs to be addressed.

I should also like to turn some attention to the generally unremarked overlap between electromagnetic vulnerability of the type described by the EMP Commission and the more general issue of cyber vulnerability. While not often considered in tandem, it is more correct to consider EMP vulnerabilities as one end of a continuous spectrum of cyber threats to our electronic based infrastructures. They share both an overlap in the effects produced – the failure of electronic systems to perform their function and possibly incurring actual physical damage – as well as their mode of inflicting damage. They both reach out through the connecting electronic distribution systems, and impress unwanted voltages and currents on the connecting wires. In the usual cyber case, those unwanted currents contain information – usually in the form of malicious code – that instructs the system to perform actions unwanted and unanticipated by its owner. In the EMP case, the impressed signal does not contain coded information. It is merely a dump of random noise which may flip bit states, or damage components, and also ensures the system will not behave in the way the owner expects. This electronic noise dump may thus be thought of as a "stupid cyber". When addressing the vulnerability of our infrastructures to the cyber threat, it is important that we not neglect the EMP end of the cyber threat spectrum. And there is another important overlap with the cyber threat. With the grid on the cusp of technological change in the evolution to the "smart grid", the proliferation of sensors and controls which will manage the new grid architecture must be protected against cyber at the same time they must be protected against EMP. Cyber and EMP threats have the unique capability to precipitate highly multiple failures of these many new control systems over a widely distributed

geographical area, and such simultaneous failures, as previously discussed, are likely to signal a wider and more long lasting catastrophe.

Another important legacy of the EMP Commission was to first highlight the danger to our electric grid due to solar storms, which may impress large - and effectively DC - currents on the long runs of conducting cable that make up the distribution system. While this phenomenon has long been known, and protected against, by engineering practices in the power industry, the extreme 100-year storm first analyzed by the Commission is now widely recognized to represent a major danger to our national electrical system for which adequate protective measures have not been taken and whose consequences – the likely collapse of much of the national grid, possibly for a greatly extended period, may rightly be termed catastrophic. At this point, the only scientific controversy attending the likelihood of our system being subject to a so-called super solar storm, is related to the time-constant. But these events have already occurred within the last century or so, they will occur again. We should be ready.

The most important legacy of the EMP Commission however, was in the recommendations which were provided that would, if acted upon, protect key assets of both the civilian and military infrastructures, And it is here that I should like to point to an important divergence in the government's response. The (classified) recommendations that were provided to the Department of Defense were formally considered, in the large main concurred with, and then acted upon. The Secretary of Defense issued a classified action plan, out-year funding was POM'd in the FYDP, an office and an official of responsibility were appointed, a standing Defense Science Board committee was stood up, an active research program is maintained, and survivability and certification instructions were issued by both DOD and by USSTRATCOM. Today, while vigilant oversight continues to be warranted, an EMP awareness pervades our acquisition system and operational doctrine. The response on the civilian side of the equation was not so rosy. The final report of EMP Commission contained seventy five recommendations to improve the survivability, operability, resilience, and recovery of all the critical infrastructures, and in particular of the most key of all, the electrical grid. Most of these recommendations were pointed towards the Department of Homeland Security. While there have been some conversations, it has been hard to detect much of an active resonance at all issuing from the Department. They have not, as far as I know, even designated EMP as a one of their ten of fifteen disaster scenarios for advanced planning circumstances. And this at a time when they do include a low altitude nuclear disaster -certainly disastrous but not one that would produce wide ranging EMP.

In the end, it is hard to deal with seventy five recommendations, all at once. But the solution is not to ignore all of them. If there is only a single essentially a no-cost step I would leave this Committee with, it would be to task the Department of Homeland

Security with responding to the still languishing recommendations of the EMP Commission. The Department of Defense did issue a response, as mandated by the legislation which originally created that Commission. But no such mandatory response was levied at the time on the Department of Homeland Security, which did not even exist when the Commission legislation was passed as part of the National Defense Authorization Act of 2001. The DHS should be required to explain which recommendations they concur with and/or with which they non-concur, and why. They should be asked to prioritize amongst the seventy five and come back with implementation recommendations, or explain why they think it is unnecessary. And finally, I would also urge the Committee to support passage of the Critical Infrastructure Protection Act.

I wish to thank the Committee for this opportunity to present my views of this most important issue.