TESTIMONY OF DR. MICHAEL J. FRANKEL

INFORMATION SUBMITTED FOR THE RECORD

HOUSE HOMELAND SECURITY COMMITTEE HEARING

CYBER SECURITY AND OTHER (EMP) THREATS TO THE POWER GRID

HOUSE CANNON OFFICE BUILDING, ROOM 311

JULY 21, 2009

My name is Mike Frankel and I served as the Executive Director of the EMP Commission for the entire span of its activities, commencing with its authorization in the Floyd Spence National Defense Authorization Act of 2001 and culminating with the delivery of our final, classified, report to the Congressional oversight committees in February of this year. Presently, I am Chief Science Officer for L-3 Communications/Applied Technologies Group. I am a physicist by training and avocation, and have spent many years developing technical expertise in nuclear weapon effects and managing WMD related programs for the Department of Defense in a career that spanned research work for the Navy, the Defense Nuclear Agency, the Defense Threat Reduction Agency, and the Office of the Secretary of Defense. The perspective of the EMP Commission is being more than adequately represented to this Committee today by our very distinguished Chairman, Dr. William Graham. I should like to submit instead complementary background information that addresses in part a topic that was not emphasized in our final report, and that is the nexus between cyber threats and EMP.

This Committee is to be commended for holding this hearing which specifically includes the full spectrum of electronic threats to the power grid. While "ordinary" cyber and EMP are not usually thought of as coupled, this has been a mistake. The cyber threat is much in everyone's consciousness with an immediacy as current as yesterday's headlines, in this case the alleged North Korean source of cyber attacks on networks in South Korea and the United States. This Committee has previously rendered valuable service by highlighting the dangerous cyber vulnerabilities of the power grid exposed in the "Aurora" test series conducted at the NNSA's Idaho National Laboratory. The EMP threat has been much less in the public consciousness to date, although the range of potential damage from such an event may, as described in the public portion of the EMP Commission's report, exceed that realizable from most cyber attack scenarios. I should like to advance the somewhat new perspective that electromagnetic pulse threats to our critical infrastructures, specifically including the power grid, need to be thought of as but a – hitherto neglected - component of the cyber security threat. More broadly speaking, there is a spectrum of electronics threats to the power grid, that range from conventional notions of cyber to different forms of EMP – both

nuclear and non-nuclear, and even natural disasters – an electronic Katrina if you will.

The nature of a cyber threat is to reach out and touch something, electronically, through its connected network. This may be thought to occur through delivery of intelligent messages which encode information and/or instructions that direct a system to some unwanted activity that may prove very harmful to its owners' interests. A SCADA may be reached and instructed to open or close a valve controlling pressures in a natural gas pipeline, with a disastrous pipeline explosion as a result. Indeed, this has already happened through SCADA malfunction, albeit not deliberately intentioned. The Aurora test series exposed by this Committee which destroyed an electrical generating system, at its base demonstrated the disastrous effects of the mischievous at-a-distance control of an electronic control system. EMP – both nuclear and non-nuclear – will also reach out and impress unwanted signals through the connected network. But in the case of EMP, the signals do not contain specific information or instructions. They are simply shot-gunned electronic pulses, without encoded information, which nevertheless, at low power levels, upon encountering vulnerable systems such as SCADAs, change their bit settings in unpredictable ways guaranteeing they will not operate as planned. Of course at higher power levels, as documented by the EMP Commission, they may cause actual physical damage to any encountered electronic system, up to the point of burning out and melting critical circuit elements. Thus, at low levels of intensity, EMP may rightly be thought of as a "stupid cyber" threat.

These hearings are also particularly timely in light of the current intellectual energy being invested in the pursuit of energy independence, in particular the development of "smart grid" technology as well as alternative energy sources such as wind and solar. While smart grid is an evolving concept and its architecture still a moving target, some outlines of its ultimate shape are emerging and it is clear that it will depend, to a much a greater degree than present, on the ability to fine tune the delivery of energy to where and when it will be needed. And this will necessitate the proliferation of more, and smarter, sensors and control systems than their already ubiquitous presence, to exercise the real time capabilities of the newer and more agile grid architecture. With such a proliferation comes enhanced vulnerabilities, to both cyber and EMP threats. Similarly, commercial introduction of new technologies, such as ultra-high-voltage – > 1000 KV - transmission line systems as has been discussed in the context of exploitation of wind power and its delivery from the point of generation to where it's needed, entails critical new vulnerabilities as well. It is appropriate, that precisely now, at the cusp of such significant technological transformation, that proper attention be paid as well to new vulnerabilities which may be introduced in the rush to innovate. The historical economic lesson from the military systems development world is that designing protection into a system from scratch is more effective and much cheaper than attempting retrofit solutions when problems are discovered later on.

Finally, I'd like to return to the theme of a spectrum of electronic threats to the power grid which merit attention, of which "ordinary" cyber is but one component. We've discussed another component as well, electromagnetic pulses due to either nuclear or non-nuclear (RF) sources. But there are also electromagnetic pulses stemming from natural events which pose a grave danger and to which the present power grid remains highly vulnerable –the "electronic Katrina" attending a very massive geomagnetic solar storm. Solar storms – fluctuations induced in the earth's magnetic field due to eruptions of charged solar matter from the surface of the sun ("coronal mass ejections" in the astronomer's language) which are flung out in the direction of the earth, are rather common events. Most are of an intensity that present no danger to anything. Some however are significantly larger and, again on a fairly regular basis, may couple electromagnetic pulse energy to long transmission lines. These induced currents are thus a natural EMP and may overwhelm and physically damage (melt) huge and hard to replace components of the electrical grid. Just such a scenario played out in the huge solar storm of 1989 which took down the Hydro Quebec company system, rendered its many millions of Canadian customers powerless, and irreparably damaged one of their multi-million dollar extremely high voltage transformers (house sized units no longer manufactured domestically and which may take up to a year to deliver following a purchase).

But those are "ordinary" events. The EMP Commission also examined the results of a "100 year storm", a Katrina analog in the world of "space weather". Such an extreme event is guaranteed to come, it is only a question of when. Indeed such storms have already visited us during the last 100 years but they occurred at a time previous to the deployment of our modern electric power grid with its long transmission lines capable of absorbing the unwanted solar EMP energy. Since the "receiving antenna" did not yet exist, except for the spectacularly unusual auroral displays – the aurora borealis was reportedly sighted near the equator – no harm was done. Absent some preparations which have not yet been taken, the next time will be very different with extraordinary permanent damage to hard to replace components and untold suffering lasting for extended periods in its wake. So taking steps to protect the system from cyber and EMP should proceed hand in hand with protection against the full spectrum of such electronic threats. And steps which are taken to protect against a singular threat should be considered from a perspective which seeks, as far as possible, solutions that confer dual or multi-benefits against a spectrum of threats. Understanding the need to approach EMP as one of a spectrum of electronically related insults and as a component of the more generalized cyber security problem, and a serious consideration of the prospects for remedies that confer multiple protective benefits, is the proper path forward to protect our uniquely valuable power grid from all electronic threats. And the time for such planning is now.

Unfortunately, it is hard to detect signs of concern, or even interest just yet on the part of those charged with reducing the vulnerability of the electric grid. Unlike

the Department of Defense which considered the (classified) recommendations of the EMP Commission report seriously and initiated certain (classified) remedial activities, it hard to detect any similar resonance to date on the part of our civilian agencies.

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