Testimony of Chris Beck

President, Electric Infrastructure Security Council

For the

Subcommittee on Cybersecurity, Infrastructure Protection,

and Science and Technology

September 12, 2012

Good morning Chairman Lungren, Ranking Member Clarke, and Members of the Subcommittee. Thank you for holding this hearing on what I consider to be one of the greatest threats to our National and Homeland Security. As many of you know, before I became EIS Council's President, I worked for this committee, focusing on Critical Infrastructure Protection and Science and Technology issues. It was through that work that I first became aware of the threats facing our critical electric infrastructures, and I found the issue to be so important that I felt compelled to focus on it exclusively.

The Electric Infrastructure Security Council's mission is to work in partnership with government and corporate stakeholders to host national and international education, planning and communication initiatives to help coordinate infrastructure protection against electromagnetic threats (e-threats). E-threats include naturally occurring geomagnetic disturbances (GMD), high-altitude electromagnetic pulses (HEMP) from nuclear weapons, and non-nuclear EMP from intentional electromagnetic interference (IEMI) devices.

EIS Council is also proud to co-host the Electric Infrastructure Security Summit Series, the annual international government / NGO summits on infrastructure security. The third annual summit took place on May 14th and 15th this year, in the United Kingdom's Houses of Parliament in London. Ranking Member Clarke was one of the U.S. bipartisan co-chairs of that event, along with Rep. Trent Franks. This summit was a gathering of senior government representatives, scientists and industry executives from 21 countries. The conclusions and recommendations that we discussed should be of great interest to this Committee. The full report has been provided to the committee as an addendum to my testimony, and I include the summary here.

SUMMARY OF MAJOR THEMES AND RECOMMENDATIONS

Defining the Issue

The Problem: Developed nations are vulnerable to serious national power grid damage from e-threats, both natural and malicious.

The Severity: The impact will range from, at minimum, a serious financial and economic crisis to, at maximum, a catastrophe that would threaten societal continuity.

The Timing: For severe space weather, the most recent events occurred 90 and 150 years ago, but the precise timing of the next such occurrence, as with all extreme natural disasters, is unknown. For malicious EMP, either local (non-nuclear) or sub-continental (nuclear), a strike could be induced by ongoing vulnerability coupled with rapidly changing geopolitical realities.

The Key Questions

1. **Should we respond to e-threats?**
Should we accept the status quo, and minimize near-term costs by accepting growing vulnerability, or begin reducing vulnerability?

2. **If we respond, what is the path?**
How should we address interconnect-wide interdependence, and how should we proceed with implementation?

3. **If we respond, who should be involved?**
Who should take responsibility to define the path, and implement it?

4. **How broad should our response be?**
Should both GMD and EMP be included?

The Response: Consensus Recommendations

1. **Should we respond?**
A common theme of the summit deliberations, broadly accepted in all presentations and discussions, was that the risks associated with severe e-threats are serious, and it is time to begin taking positive actions to protect critical infrastructures.

2. **What is the path?**
The broad consensus of summit presenters and other delegates was that we need to establish interconnect-wide standards and plans. For implementation, we should begin working aggressively to validate and implement specific protection measures, while also pursuing expanded modeling, priority assessment and planning. More specifically:

> **a. Define and apply interconnect-wide standards and protection plans**
> We should define and apply applicable interconnect-wide e-threat protection standards, through regulatory or other means, and develop implementation plans that include prioritized protection for critical assets.

b. Pursue two paths to implementation:

1. Validate and implement specific, cost effective protection measures.

We should thoroughly evaluate protective measures to validate that they support the e-threat standards, including both procedural and hardware-based measures (e.g., transformer or other hardware design upgrades, current blockers, series capacitance and power substation IEMI protection).

If expectations for high effectiveness and low cost hardware-based protection can be tested and demonstrated, this will become a core approach to mitigation, beginning with development of interconnect-wide protection planning.

2. Prioritize scope and timing of protective measures by expanded hardware and interconnect-wide modeling, prioritization and data collection.

We should also pursue a path of data collection, hardware vulnerability modeling and grid impact modeling, and define critical, high value asset protection priorities. This process will guide and prioritize cost effective implementation measures. It will be even more vital in those cases where more expensive measures are needed.

3. Who should be involved?

The sense of summit presenters and delegates was that assembling and implementing a plan for e-threat protection will require the broadest possible participation among government agencies, commercial power suppliers, insurance companies and other stakeholders, each contributing in its own domain of authority and expertise. A common theme of all the discussions: The need to work toward international partnerships in developing these plans.

4. Addressing EMP and IEMI: How broad should our scope be?

These recommendations, it became clear, will be essential for both aspects of e-threats, both natural – Severe Space Weather, and malicious – IEMI and EMP. In fact, another common theme at the summit was that, in focusing on space weather, there has been insufficient attention given to the needs for protection against malicious EMP and IEMI threats. In this regard, all the security-related speakers were quite clear: Security forces cannot perform their national security and protection mission without the partnership of commercial power suppliers, who will need to "expand their resilience into a new hazard environment." The hope that the government could handle either the natural or malicious threat domain on its own was rejected, with the clearest articulation of this reality coming from speakers who represented the responsible government departments and agencies.

This summary of summit consensus-based themes and recommendations reflects many detailed comments made in the presentations and discussions during summit events. I would welcome the opportunity to discuss any of these points in greater detail.

I should note that there appear to be no significant technical or financial barriers to mitigating this threat – the technologies needed are well understood, and the cost – based on both government estimates and recent corporate experience – is quite low, even in comparison with just existing logistics and maintenance budgets for affected equipment. Rather, the primary needs seem to be for education to increase awareness and willingness to address the problem, and for coordination to address the complex government and corporate administrative structures of even the most critical infrastructures.

This concludes my prepared testimony, and I'd be happy to answer any questions.