**Testimony of Chris Beck**

**Vice President for Policy and Strategic Initiatives,**

**Electric Infrastructure Security Council**

For the

**Subcommittee on Cybersecurity, Infrastructure Protection,**

**and Science and Technology**

May 8, 2014

## Introduction

Good afternoon Chairman Meehan, Ranking Member Clarke, and Members of the Subcommittee. Thank you for holding this hearing on one of the most significant threats to our National and Homeland Security. As many of you know, before I joined EIS Council, 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 improve infrastructure protection against electromagnetic threats (e-threats) and other hazards. 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 – the focus of today's hearing.

## EMP - Defining the Issue

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

**The Severity:** The impact can range from a broad regional blackout with serious economic consequences to, in the worst case, a catastrophe that would threaten societal continuity. With even the most benign scenarios projecting high societal costs, the Committee is correct to focus on this as an issue deserving serious attention.

**The Timing:** For severe space weather, the most recent events occurred roughly 90 and 150 years ago, but the timing of the next such occurrence, as with all extreme natural disasters, is unknown. Either local (non-nuclear) or sub-continental (nuclear) EMP could occur at any time, encouraged by ongoing vulnerability, and triggered by changing geopolitical realities.

## Key Questions

1. **What should our national strategy be?** At top level, there are two alternative paths:

   a. Hope for the best: Accept the status quo.
      i. For severe space weather, this means hoping the most optimistic projections will turn out to be correct, and the impact will not be catastrophic.
      ii. EMP has been called, "The most powerful asymmetric weapon in history." This approach means hoping no terrorist organization or rogue state will ever take advantage of the power of such devastating weapons.

   b. The other alternative:

   Encourage cost-effective resilience, restoration and response planning.

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? How should the balance between public mandates and private, corporate initiative be determined?

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

## Consensus Recommendations

1. **Hope vs Preparation: Choosing a strategy.**

A common theme of all the many government reports studying these risks, also reflected in the deliberations of the Electric Infrastructure Security Summits over the last several years, is that the risks associated with severe e-threats are serious. It is hard to find anyone who would assert that, in today's world, "hoping for the best" is a good strategy for GMD, EMP or IEMI.

2. **What is the path?**

Our national power grid is organic in design, but administratively complex. This means approaches are needed that address both of these factors.

- Organization and coordination: Given the grid's organic design, the consensus of government studies is that coordinated planning and standards will be important. Finding the best possible balance between broadly accepted, pro-active corporate coordination and government action will be important to assure fast, effective progress in achieving an e-threat resilient grid.

- Technical: A key point, not always recognized, is there is no need to "gold plate" the system.

  For Severe Space Weather, there is already growing discussion of a range of strategies, and none of the approaches under active discussion – from planning measures to comprehensive automated hardware protection – appear high in cost, relative to existing logistics budgets and investment models.

  For EMP, protection planning can focus – not on hardening every component in the power grid – but on protection of a fraction of grid facilities and hardware. In other words, enough resilience investment, and associated restoration planning, to protect enough generation resources and critical loads to allow for both effective restoration and for prioritized support to critical users and installations.

## 2. Who should be involved?

Given the likelihood of a large regional power outage after a natural or malicious e-threat, power companies will need to be operating in an environment of extensive response and recovery support from federal and state government authorities, as well as community-response NGOs. Thus, the evolution of planning to address these concerns should include the broadest possible involvement of all of these stakeholders, each contributing in its own domain of authority and expertise.

## 3. How broad should our scope be?

For all the E-threats under consideration here, efforts at protection, if they are to be effective, must primarily be focused where the impact will occur – in the power grid. For severe space weather, there is clearly no other alternative. For malicious threats, EMP and IEMI, U.S. and allied government security officials and experts at the highest levels agree that neither deterrence nor active military measures can alone guarantee the security of our homeland against a determined aggressor prepared to use such weapons.

In conclusion, I should note that there appear to be no significant technical or financial barriers to mitigating this threat. The technologies and operational procedures needed are well understood, and the cost – based on both government estimates and recent corporate experience – is reasonable. One of the primary needs is for education to increase

awareness and therefore willingness to address the problem, and for coordination to address the administrative complexity of our nation's power grid.

This summary of consensus-based themes and recommendations reflects, I believe, not only the conclusions of the many major government studies of these issues, but also the deliberations of the past four international Electric Infrastructure Security Summits, with participation by the highest levels of many departments and agencies of the U.S. and allied governments, and of a broad range of scientists and domain experts working in this field

I would welcome the opportunity to discuss any of these points in greater detail.

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