EIS SUMMIT

International Infrastructure Security **Roadmap**

Edition: April 11, 2011

ELECTRIC INFRASTRUCTURE SECURITY SUMMIT

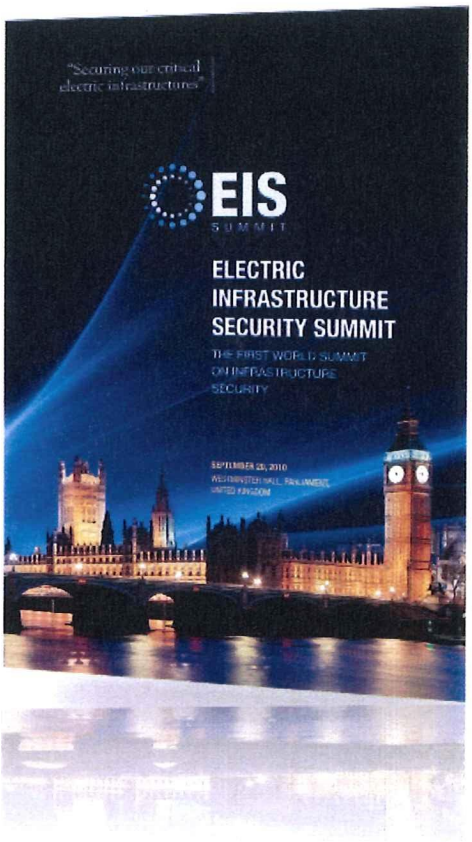
Monday, April 11, 2011
The Capitol Building
US Congress, Washington D.C.

"Securing
our critical
electric
infrastructures"

Background

At EISS London, the 1st world summit on infrastructure security, eighteen nations inaugurated a new international infrastructures security framework, focused on coordinated effort to protect against severe electromagnetic threats to national electric grids and other critical infrastructures.

The focal point of this effort is the developing International Infrastructure Security Roadmap, which lays out a milestone-driven plan designed to encourage concrete progress in infrastructure protection.



About the Roadmap

Roadmap objective: The International Infrastructure Security Roadmap is designed as a hub for international cooperation in addressing severe electromagnetic threats to national electric grids and other critical infrastructures.

Two infrastructure protection categories: The Roadmap addresses two categories of infrastructure protection. General Infrastructure Protection addresses the common aspect of Severe Space Weather and EMP (both nuclear and non-nuclear), where the protection needed is the same for both threats. EMP-Unique Infrastructure Protection addresses the unique aspect of nuclear and non-nuclear EMP threats, as a sub-category of the Roadmap.

Government and industry paths: The Roadmap includes two recommended milestone plans, or paths – one for government regulators and legislators and one for private industry, including both bulk power suppliers and providers of other critical infrastructures.

An interactive process: A successful Roadmap must provide for effective interaction between government and industry paths. While regulators and legislators define overall objectives and requirements, implementation is typically the domain of private industry. Thus, requirements must be informed by implementation options and constraints, while implementation choices will need to respond, in turn, to government assessment of adequacy in meeting objectives. The Roadmap provides this interaction with feedback ramps, connecting the government and industry paths at key milestones.

Roadmap Stakeholders: Typical government and industry stakeholders important to the Roadmap process. [The example shown is for the United States]

Roadmap Editions
- EISS Executive Steering Committee
- EISS Working Group

Roadmap stakeholders

Editions of the evolving International Infrastructure Security Roadmap are developed by the EISS Working Group, based on review by the EISS Executive Steering Committee. While the Roadmap is designed to provide for parallel, interactive government and industry paths, development and evolution of an effective plan must be responsive to a full set of government and industry stakeholders.

Government concurrence

One of the keys to a successful Roadmap process is planning for all government and industry stakeholders to have input in its development, helping ensure the Roadmap meets critical objectives with a well-defined plan that has the buy-in of regional and national regulators, government departments and legislators.

Defining objectives

Thus, top level objectives will be defined by regulatory authorities in coordination with legislators and appropriate government departments, and with input from the power industry and other key stakeholders[1].

1 For the United States (see figure above), these objectives are expected to be defined by the Federal Energy Regulatory Commission (FERC) in coordination with Congress and with the Department of Energy, the Department of Defense and the Department of Homeland Security, with input from:
- The North American Electric Reliability Corporation (NERC) and the power industry
- The National Association of Regulatory Commissioners (NARUC) and State and local utility commissions
- Protection technology suppliers

Enabling early power industry investment

Commitment to these objectives by government regulators and legislators will be vital to give power industry decision makers the confidence to take early, independent steps toward grid protection without concern that legislative or regulatory language will undercut such investment. At the same time, early involvement of power industry representatives as well as protection technology suppliers will help ensure objectives are realistic and effective.

Peer review

To help build confidence throughout the process, peer review from subject matter experts in both the private and public sectors (including national laboratories) should be available, as needed, for government decision makers.

Roadmap content

International applicability: The EISS Roadmap is designed to provide for international participation. Where specific examples are needed, member nation infrastructure networks will be used as templates and case studies.

Interactive and evolving: As an evolving document, each new edition of the EISS Roadmap will reflect a current iteration of a developing, interactive process. In that regard, the top level objectives and milestones defined below represent only the Roadmap's starting configuration. As this effort proceeds, the high level milestones below will both change and become increasingly detailed, to help characterize well-defined steps that can guide the next set of government and industry milestones. At a later phase, more detailed milestones will include elements of scheduling dependencies, schedule constraints and resource requirements.

Scope: This roadmap is designed to allow addressing infrastructure security in stages. At this stage, the Roadmap is designed to address security of highly critical infrastructures: National electric grid, water supply, sewage and communication systems. Over the long term, other infrastructure systems may be added and addressed.

Benchmark threat scenarios: Top level objectives and milestones address protection requirements for design-case benchmark scenarios, to be defined early in the Roadmap process.

1.0

Top level objectives

Required End State: Electric grid highly resilient to severe space weather and EMP

- **Non-catastrophic failure:** During a severe space weather or EMP event, grid components will not suffer damage that will lead to long term, wide area blackouts.
- **Rapid recovery:** In the wake of a severe space weather or EMP event, grid operation will be restored in most areas in times comparable to those experienced in recent wide area blackouts.

Objectives

Top level objectives address the Required End-State for both General Infrastructure Protection and EMP-Unique Infrastructure Protection, except as noted

Objective 1.1: Automated protection

Integrated hardware-based protection ("hardening") permanently integrated into the grid. Once in place, human intervention is not required to protect grid components. Examples: Ground-induced current blockers, Faraday cages with through-put protection, surge arrestors, and optical couplings.

Scope:

- Essential long lead components for the Grid or other highly critical infrastructures– e.g., High Voltage Transformers, Generators
- High failure rate components – Components expected to potentially fail in large numbers, where failure rates significantly exceed available spares, or exceed levels susceptible to reasonable replacement times (e.g., failure rates much higher than can be found and replaced by existing support teams)
- Components needed to allow response teams to find and resolve problems in reasonable times.

Objective 1.2: Maintaining adequate spares.

In cases where component failures are expected even after Grid hardening, adequate spares must be pre-positioned to allow the grid to return to normal operation.

Note: Providing a special stock of spares is an acceptable mitigation only where hardening is impractical AND existing support teams are judged sufficient to locate and replace the full expected range of failed components, using the limited grid status / diagnostics indicators expected to be available.

Scope:

Components for which: 1) Spares can be provided in numbers required for possible failure rates due to benchmark threats, AND 2) Possible failure rates are consistent with finding and replacing / reconfiguring components and networks in reasonable time with existing support teams.

Objective 1.3: Manual procedure-driven protection

Severe Space Weather warnings can allow for operational hardening approaches that can be helpful, if complementary to automated, hardware-based protection.

Scope:

- Operational means of protection for critical grid components when used synergistically with hardware based approaches.
- Systems, subsystems and components that can be taken off line or otherwise protected for all warnings of threats that could reach benchmark levels – including many expected false alarms – without significant reduction in performance performance of the Grid or other highly critical infrastructures.
- Networks or sub-networks that could be disconnected from the larger Grid and run autonomously, often called "islanding".

2.0 Roadmap Milestones – Government Path

(Example based on U.S.)

Note: Key to numbering – Numbers ending in "IF" refer to "Industry Feedback."

2.1 Technology Sharing: Plan for Technology Transfer among EISS Partner Nations

2.2 Defining Detailed Requirements:

2.2.1 Regulators to work with technical team to define design-case benchmark scenarios

2.2.2 Build and test prototypes of technologies needed

2.2.2.1 General Infrastructure Protection

2.2.2.2 EMP-Unique Infrastructure Protection

2.2.2-IF – Seek input from Protection Technology Companies on prototype options

2.2.3 Define top level objectives, including:

2.2.3.1 Critical Hardware List

2.2.3.2 Solution menu of validated hardware and process solutions for General Infrastructure Protection

2.2.3.3 Solution menu of validated solutions for EMP-Unique Infrastructure Protection

2.2.3-IF – Seek Industry Feedback

2.2.4 System Engineering – Infrastructure Protection Planning Program: Develop an Annotated Critical Hardware List

Match the Critical Hardware List with recommended hardware and process solutions from the Solution menu to create an

endorsed Annotated Critical Hardware List

In particular: For one or more example National Grids, based on system models and analysis, recommend optimum hardware and process solutions for different components and subsystems

2.2.4.1 General infrastructure protection

2.2.4.2 EMP-Unique infrastructure protection

2.2.4-IF – Seek Industry Feedback

2.3 Implementation Planning

2.3.1: Develop national implementation plan

2.3.1.1 General Infrastructure Protection

2.3.1.2 EMP-Unique Infrastructure Protection

2.3.1-IF – Seek Industry Feedback

2.3.2: Develop example regional and local implementation plans as recommended templates for government and private industry

2.3.2.1 General Infrastructure Protection

2.3.2.2 EMP-Unique Infrastructure Protection

2.3.2-IF – Seek Industry Feedback

2.3.3: Local and regional plans are reviewed and endorsed by regulators

2.4: Implementation

2.4.1: Government to review power and other critical infrastructure companies' implementation plans.

2.4.2: Federal regulators monitor implementation

3.0

Roadmap Milestones – Industry Path

(Example based on U.S.)

Note: Key to numbering – Numbers ending in "GE" refer to "Government Endorsement."

3.1. Defining Detailed Requirements:

3.1.1: Protection Technology Companies propose prototype protection options

3.1.1.1 General Infrastructure protection options

3.1.1.2 EMP-Unique Infrastructure protection options

3.1.2: Bulk Power suppliers and Grid companies recommend:

3.1.2.1 Critical Hardware List

3.1.2.2 Solution menu of hardware and process solutions

3.1.2.2.1 General Infrastructure Protection solutions

3.1.2.2.2 EMP-Unique Infrastructure Protection solutions

3.1.2-GE – Seek Government Endorsement of proposed hardware and process solutions

3.2: Implementation Planning

3.2.1: Review National Implementation Plan

3.2.2: Industry power suppliers and related companies to develop implementation plans

3.2.2.1 General Infrastructure Protection

3.2.2.2 EMP-Unique Infrastructure Protection

3.2.2-GE – Seek Government Endorsement

3.2.3: Power suppliers work with Local and regional utility commissions to adapt example plans for their own systems

3.2.3.1 General Infrastructure Protection

3.2.3.2 EMP-Unique Infrastructure Protection

3.2.3-GE – Seek Government Endorsement

3.3: Implementation

3.3.1: Power companies implement protection plans.

3.3.1.1 General Infrastructure Protection

3.3.1.2 EMP-Unique Protection

3.3.1-GE – Seek Government Endorsement

4.0 Streamlined Milestones

(Example based on U.K.)

4.1 Risk Identification: Identify that the risk from severe space weather may be greater than previously thought

4.2 Benchmark Scenario Selection: Decide on worst credible scenario that should be considered

4.3 Impact Modeling: National Grid to estimate the consequences of the worst credible scenario on the transmission network.

4.4 Impact Assessment: DECC/Ofgem/National Grid consider the findings and in particular whether the potential consequences are acceptable or not.

4.5 Mitigation Planning: DECC/Ofgem/National Grid consider how the grid could be protected and the standard of protection that should be provided. This assessment to include both investment options (e.g. blocking capacitors or protection schemes) and operational actions (e.g. switching out transformers that are particularly at risk in response to a warning).

4.6 Grid Upgrade Design: National Grid design and cost protection scheme for grid

4.7 Design Review: Review National Grid's scheme and challenge costs as appropriate. (This could be as part of a Price Control Review, or done separately)

4.8 National Grid Response: National Grid accept Ofgem's proposed funding mechanism (or refer to Competition Commission)

4.9 Implementation: National Grid install protection to the agreed level, with DECC and Ofgem monitoring progress.

DATOS TÉCNICOS SOBRE FENÓMENOS SOLARES

A.- FULGURACIÓN SOLAR

Causa: Emisión por parte del sol de rayos X y/o rayos ultravioleta que provoca una radiación electromagnética de llegada inmediata a la tierra (segundos) y con una duración que puede ir de minutos a una o dos horas.

Efectos: Puede producir desde perturbación en las señales de radio y debilitamiento de las ondas cortas de radio, hasta la afección a la radiocomunicación de tierra y navegación por satélite, e interferencias de radar.

Medidas preventivas: Emisión por radio en frecuencias bajas.

Sectores afectados: Comunicaciones de radio terrestres y vía satélite.

B.- TORMENTAS DE RADIACIÓN SOLAR

Causa: Provocan Eyecciones de Masa Coronal, consistentes en emisiones de partículas solares de alta energía (eventos de protones o neutrones), las cuales pueden llegar a la zona terrestre en pocos minutos o horas y con una duración de varios días.

Efectos: Pueden afectar físicamente y al normal funcionamiento de los satélites provocando lecturas de posición y medida erróneas, así como a los vehículos aeroespaciales, a las aeronaves (alta dosis de radiación) y un debilitamiento de las ondas cortas de radio.

Medidas preventivas: Uso de estructuras y componentes electrónicos resistentes a la radiación, así como reducir el número de vuelos de aeronaves en rutas polares.

Sectores afectados: Aeroespacial, transporte aéreo y equipos y comunicaciones vía satélite.

C.- AGUJEROS CORONALES

Causa: Emisión de partículas de media-baja energía, provocando tormentas geomagnéticas que ocasionan corrientes geomagnéticas inducidas, pudiendo llegar a la tierra entre dos y cuatro días y con una duración de días.

Efectos: Producen afección al sistema eléctrico (subestaciones, centros de transformación y redes de alta tensión), corrosión en la red de oleoductos y gasoductos, disrupción de cables de telecomunicaciones y efectos en componentes electrónicos.

Medidas preventivas: Protección de generadores de plantas nucleares así como subestaciones y centros de transformación eléctrica, suministro eléctrico auxiliar (grupos electrógenos, cámaras Faraday, transformadores de sustitución), etc.

Sectores afectados: Sistema eléctrico, con interdependencias con otros sectores como el del transporte.