EIS SUMMIT IV

Summit Report

EISS IV | Resilience and Synergy

Electric Inffrastructure Security Summit

Washington D.C., 2013

THE FOURTH ANNUAL WORLD SUMMIT
ON INFRASTRUCTURE SECURITY

“

That's why these robust public-private partnerships are so important to help secure these essential infrastructure services from hackers, criminal terrorists, major storm events, and other adversaries. And that's why this conference is so important.

Daniel Poneman, Acting Secretary,
U.S. Department of Energy,
speaking at EISS IV, Washington D.C.

Electric Infrastructure Security Summit IV Washington D.C.

The fourth annual world summit on infrastructure security

Hosted as an international government, industry and NGO partnership, the EIS Summit Series provides a broad framework for addressing critical infrastructure vulnerabilities. Focusing on threats that could lead to extended, wide area power outages and cascading infrastructure failures, EISS IV moved from assessments of current status to recommendations for next steps that could enhance grid security against multiple hazards.

May 20-21, 2013 • The Capitol Building US Congress, Washington D.C.

OVERVIEW

Organizing Co-Chairs of the EIS Summit Series. From left: Rt. Hon. James Arbuthnot MP, Rep. Yvette Clarke (D, NY), Rep. Trent Franks (R, Az)

OVERVIEW

EISS IV, the fourth annual world summit on infrastructure security, brought together senior government representatives, scientists, energy sector executives, insurance corporation managers and other key stakeholders from the United Kingdom, North America, Israel and Europe. The theme for the summit was "Resilience and Synergy," and the sessions focused on leveraging common approaches for power grid protection. Summit delegates discussed risks of extended outages from severe space weather, EMP, Cyber and other "Black Sky Day"[1] hazards.

As an input to the discussions, the summit began with a review of some of the most important government studies on E-threats. In the last decade, U.S. Congressional Commissions and studies by the Department of Energy, the Pentagon, the Federal Energy Regulatory Commission, NASA, the National Academy of Sciences, DHS and other federal agencies all projected growing, unprecedented risks of catastrophic infrastructure failures due to such threats, on subcontinental scales. More recently, Insurance and re-insurance corporations, responding to their own risk assessments, have also begun calling for increased action to address these hazards.

With plans in place for serious grid expansion and with growth projected for malicious threats, vulnerability is increasing. Government and industry representatives addressed improved grid resilience and security as urgent priorities, and reviewed important first steps – and next steps – that address them.

The common conclusion: In the coming years coordinated, expanded effort will be needed, if we are to achieve high-confidence grid protection from events that could have severe societal impact.

EIS SUMMIT SERIES ORGANIZING CO-CHAIRS

The Rt. Hon. James Arbuthnot MP, U.S. Congresswoman Yvette Clarke, U.S. Congressman Trent Franks. Honorary Co-Chair: Lord Toby Harris.

The Electric Infrastructure Security Summit Series is an international government / industry / NGO partnership, hosted by the Electric Infrastructure Security Council and the Henry Jackson Society.

SPONSORS FOR EISS IV WASHINGTON D.C.

Organizations – United States Department of Energy; North American Electricity Reliability Corporation; Lloyd's; Emprimus.

Foundations and Individuals – Dr. Jack Templeton; The Newton D. and Rochelle F. Becker Foundation; Steve and Rita Emerson; The Michael and Andrea Leven Family Foundation; Kharlene and Chuck Boxenbaum; Steven and Bonnie Stern; Kenneth and Nira Abramowitz

1 "Black Sky Day" – Definition: Extraordinary and hazardous catastrophes utterly unlike the blue sky days during which utilities optimally operate

EXECUTIVE SUMMARY

On May 20 and 21, 2013 in the U.S. Capitol Building, Washington D.C., government officials and executives of energy and insurance corporations from twenty-three nations came together at EIS Summit IV – the Fourth Annual World Summit on Infrastructure Security. The summit reviewed status and next steps to improve resilience against hazards that could stress national power grids far beyond any precedent in modern times, risking severe, extended duration power outages.

The Keynote Speaker at the two-day summit was Acting Secretary of Energy **Daniel Poneman**.

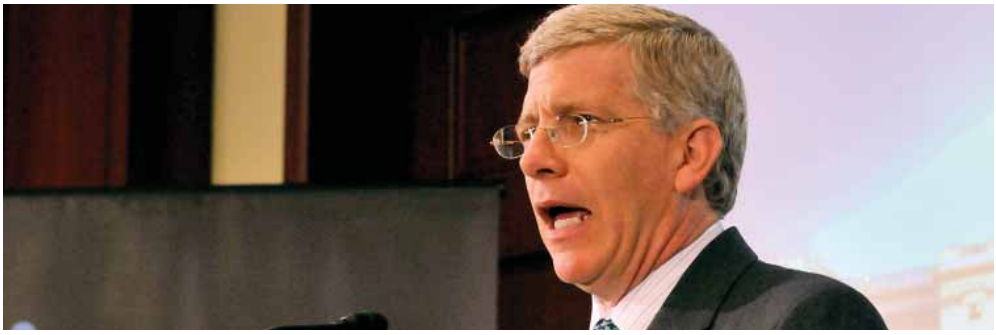
A number of other senior officials spoke at the summit.

PARTIAL LIST OF SENIOR SPEAKERS

- Deputy Assistant Secretary **William Bryan**, U.S. Department of Energy
- Deputy Undersecretary **John Conger**, Department of Defense
- Commissioner **Cheryl LaFleur**, U.S. Federal Energy Regulatory Commission
- **Jane Holl Lute**, recently Deputy Secretary of the Department of Homeland Security
- **Andrew Miller**, Chair of the U.K. House of Commons' Science and Technology Committee
- U.S. Rep. **Ed Royce**, Chairman of the House Foreign Affairs Committee
- Dr. **Paul Stockton**, former U.S. Assistant Secretary of Defense
- Dr. **Shlomo Wald**, Chief Scientist in Israel's Ministry of Infrastructure, Energy and Water Resources

Summit Organizing Co-Chairs

- U.S. Rep. **Trent Franks (R, AZ),** Chairman of the Congressional Electromagnetic Pulse Caucus
- U.S. Rep. **Yvette Clarke (D, NY),** the top Democrat on the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
- The Rt. Hon. **James Arbuthnot** MP, Chair of the U.K. House of Commons' Defence Committee.



Daniel Poneman, Acting Secretary of Energy

Coordinated planning

One of the most important messages from speakers and discussion was the need for coordinated planning and effort, within and between both the industry and government sectors. While public energy policies and interests are formalized and expressed by administrative and legislative government bodies, NGOs and public interest groups, the power grid itself is almost exclusively in private hands. This makes public – private partnerships crucial to progress in addressing “Black Sky Days.”

This point was highlighted by Acting Secretary of Energy Daniel Poneman.

"The federal government wants to be a strong partner, and I emphasize the word partner in dealing with these threats. But we also understand that government doesn't have all the assets, doesn't have all the resources, doesn't have all the answers. And therefore, perforce, we're going to need to work -- the Executive Branch is going to need to work – with the Congress; the federal government is going to have to work with the states and localities; and all of us are going to have to work with industry, whether it's investor-owned utilities or world cooperatives or public power companies.”

“Everybody's got their role to play. In the United States, again I'm sure everyone here knows the private sector owns 85% of our critical infrastructures, including transportation, communications, and electric power systems. That's why these robust public-private partnerships are so important to help secure these essential infrastructure services from hackers, criminal terrorists, major storm events, and other adversaries. And that's why this conference is so important."

"The US Department of Energy stands ready to continue our partnership and to help however we can in protecting the nation and advancing these critical goals, for our generation and all that follow."

“Window of Opportunity”

The primary strategies for addressing severe threats,speakers concurred, must be broadly-based: energy sector, private, public-private, multi-sector and international. As many speakers pointed out, though important steps have begun in some of these domains, progress with such a wide array of players is not easy. How wide is the “window of opportunity” to capitalize on these initial steps?

Rep. Franks answered the question this way:

“[T]here is that moment in the life of nearly every problem when it is big enough to be seen, and still small enough to be addressed by reasonable people and to be solved. And I believe you and I live in that moment when there still may be time for the free world to address and mitigate this vulnerability that naturally occurring or weaponized EMP represents to the mechanism of our civilization.”

The common goal: Cost effective resilience

In the plenary sessions and in roundtable discussions, scientists and government and industry leaders highlighted the need to address severe, Black Sky Day threats. The enormous costs and catastrophic impact of potential manmade or natural threats were seen to far outweigh the relatively modest costs projected for coordinated, basic steps toward protection. An event that left much of a nation without power for an extended duration would have a shattering impact on society, families and individuals throughout the affected area – from severe dislocation to health emergencies and loss of life, and risks to community safety and security. In comparison, basic, coordinated, multi-sector measures for power grid resilience and restoration could focus – not on building a “gold-plated” zero-risk grid – but on providing for recovery over acceptable timelines, at modest, sustainable costs.

Increasingly, there are notable examples of private sector initiatives to plan and implement enhanced resilience for Black Sky Day hazards. This is true particularly in sensitive regions in the United States, but examples were also given for power companies serving allied nations. And at the same time, several companies are now developing and testing new products to aid in achieving enhanced resilience.

In parallel, in the United States and elsewhere, government representatives from Washington, London, and Jerusalem said that legislative or regulatory protective measures are increasingly being considered, and in some cases (as with FERC's Final Rule On Reliability Standards For Geomagnetic Disturbances, issued just before the summit) have already been taken. Government agencies, such as the U.S. Department of Defense, are also developing policies to reduce their own vulnerability to an extended power grid failure.

Ideally, corporate initiatives, in combination with industry-coordinated government steps, could provide opportunities for collaborative action by corporate power grid asset owners interested in investing in improved resilience against E-threats and other severe hazards.

Resilience and Synergy

Overall, government and industry speakers broadly agreed that they need to work together to develop a better-protected grid – to carefully consider options for policies, plans and both new and traditional operational and hardware options that could improve resilience and recovery from a Black Sky Day natural, manmade or malicious event. Synergistic steps, in particular, were highlighted – where measures taken to protect against one hazard (e.g., a stressing cyber attack) could make the grid less vulnerable to others (e.g., severe space weather or EMP).


STOP

SESSION I

SECURITY, RESILIENCE AND SYNERGY – STRATEGIC PERSPECTIVES

With participation by 23 nations, government and corporate sector energy stakeholders spoke of the need for broader education, communication and coordination in addressing severe emerging hazards, and for definition of cost effective, rational measures to mitigate the consequences of such hazards. Nevertheless, many speakers pointed out that progress in these areas has begun taking shape, with improvements in awareness and notable examples of corporate and government steps to provide resilience for "Black Sky Day" events.

Improving Awareness – Recognizing Black Sky Day Hazards

Severe, emerging or newly recognized threats to national power grids have become part of the broadly accepted risk / resilience balance dialogue. First steps toward improved education, coordination and threat assessment for emerging risks are beginning to take shape in initiatives pursued by industry leaders, while government agencies explore options for broader, coordinated measures.

Severe Space Weather

As national power grids grow and evolve, we face the potential for increased vulnerability to severe space weather and related hazards, and for large regional blackouts of unprecedented reach and duration – the Black Sky Day scenario. Studies projecting the potential for Severe Space Weather and other emerging threats to evolve into such a scenario have sparked energy infrastructure security planning in the U.S. Department of Defense, focused resilience investments by concerned companies, and both legislative and regulatory initiatives.

Malicious Threats

Speakers spoke of several emerging risk areas related to malicious threats, including severe cyber-attacks, Intentional Electromagnetic Interference (IEMI) Weapons, and Nuclear EMP. Domain experts at the summit, speaking of these different malicious threat vectors, spoke of increasing threat levels.

For example, in regard to nuclear EMP, proliferation is seen as a growing risk, with an increasing trend of hostile or unstable powers on a path that could lead to developing nuclear weapons. Of the many concerns raised by such proliferation, the most serious may be the growing threat of electromagnetic pulse (EMP) attacks that could shut down all or part of a nation's (unprotected) power grid for months, if not years.

China and Russia have developed and deployed "super-EMP" or "no-yield" nuclear weapons, with greatly enhanced effectiveness and range. There is also evidence that experts from one or both nations have helped North Korea and Iran in their nuclear and missile programs. North Korea, according to Russian sources quoted at the summit, may have used this expertise to design or build-in EMP-enhancing technology in developing nuclear warheads. Iranian officials have reportedly attended all three of North Korea's nuclear tests.

Several speakers referred to the rapid growth of non-nuclear EMP weapon development, a weapon technology now considered near deployment threshold for an expanding number of countries. Curtis Birnbach, President of Advanced Fusion Systems, referred to test programs that have demonstrated, over short ranges, non-nuclear electromagnetic pulses even more powerful than super EMP weapons. These devices can be portable and inexpensive, enabling an adversary to simultaneously attack multiple power grid targets at different locations.

The above "EMP Suitcase," displayed at the summit, is available for purchase in the U.S. as electrical test equipment. This and related devices on the open market represent a risk of highly accessible non-nuclear EMP weapons. Display courtesy of EMPRIMUS.

Societal Impact
The need for a "systems approach"

While there have been many examples of relatively short, limited-area power outages, the developed world has no experience with an extended duration, nationwide or large regional power outage. The integrated, national-scale power grids we take for granted first appeared much less than 100 years ago, and the societal impact of emerging Black Sky Day threats has no precedent. Awareness of the consequences of such an event is not nearly as mature as for severe storms, earthquakes or other more common, if less devastating, catastrophes.

The remarkable advantages of ubiquitous, versatile electric power have brought modern societies to the point where essentially 100% of critical, life-sustaining infrastructures require uninterrupted, high quality electric power. The implications of a long term outage are devastating – with the potential for cascading infrastructure failures that could leave much of a nation without the means for sustaining life, health and civil well-being. This means addressing this issue will require a "systems approach," ultimately including impacts that extend well beyond the power grid. As planning becomes more mature, many different sectors of society will be involved in working to assure resilience.

"When the electric grid goes down," said **Patrick J. Natale**, Executive Director of the American Society of Civil Engineers, "the water purification plants close. […] So one thing interacts with another." That is why, he said, "We need to look at the systems approach to this whole issue of where we're going."

"I believe one of the advantages of this holistic approach of de-stove piping and looking across will allow us to see: Some of the things we could do to address EMP could help us on GMD, could help us on cyber security, can help us on resilience, can help us on efficiency."

Daniel Poneman,
Acting Secretary, U.S. Department of Energy

"We need to continue to stay engaged on an international basis. […} When US forces are deployed abroad, in partnership with many of the nations represented here, we need to always be mindful that … EMP poses a global threat as well."

Dr. Paul Stockton
former U.S. Assistant Secretary of Defense

"I have a four billion dollar a year utility bill, and I would like to make sure that we continue to receive service."

John Conger
DOD Deputy Undersecretary

Making progress

All societal sectors represented at the summit – government, corporate and NGO – spoke of an increasing focus on developing plans to address these threat domains.

The Government Sector

Within U.S. government agencies, increasing attention is being given to energy security. The U.S. Department of Defense (DoD) has created, and is now implementing, its first-ever Mission Assurance Strategy. It is designed to ensure DoD is prepared for asymmetrical threats that could cripple the domestic infrastructure on which both U.S. and overseas operations depend, according to **Dr. Paul Stockton**, former Assistant Secretary of Defense.

"We need to be prepared," he said, "not only for the typical kinds of military threats against the United States, not only challenges to our deployed forces abroad, but to deeply asymmetric ways that adversaries might attack us."

While other federal agencies are also taking a closer look at their own energy security issues, Acting Energy Secretary Daniel Poneman spoke of the need for government stakeholders to take a broad approach, addressing severe risks to the power grid by breaking down government "stove-piping." Among other advantages, he explained, this can help in designing resilience measures that can address multiple hazards.

John Conger, the Deputy Undersecretary for Installations and Environment at DOD, said the department is crafting a strategy to operate during a mid-level outage of 30 days. He has advised base commanders to work with local utilities on their power restoration plans, to ensure the base is assigned a high priority for power restoration. From a community perspective, this could be an important recovery strategy for any such emergency, since that base could become an effective staging area to support the entire region.

The Corporate Sector

In the energy sector, work is going on to implement and evaluate mitigation strategies for threats to the power grid. **John Houston**, Senior Vice President of CenterPoint Energy in Houston, described the extensive work CenterPoint is doing to evaluate GMD vulnerability, and to harden Control Centers against EMP E1. **Frank Koza**, Executive Director of Operations Support at PJM Interconnection, predicted that, within a year, the industry may be ready to prioritize equipment to deploy for mitigation.

At the same time, several companies are now in the final stages of developing specialized equipment for protection of high value grid assets against space weather and EMP effects. For example, both Emprimus and Advanced Fusion Systems plan to manufacture and distribute "current blockers," for protection of critical transformers against large, damaging Geomagnetically Induced Current (GIC). Advanced Fusion has also just completed work on a large new test facility, with the capacity to duplicate EMP or Severe Space Weather waveforms. The company announced it will conduct tests for any company – including a competitor – working to protect the grid.

NGO Roles

Non-Government Organizations can have unique roles in helping leverage corporate and government efforts. By fostering communication and hosting planning opportunities, EIS Council has worked with its partners to help catalyze corporate, multi-sector, government and international coordination.

"I would be the first to tell you that I don't think the operating procedures we have are going to get us through the really extreme space-weather events. […] I think I can tell you now that the industry gets it.

We understand that this is a serious issue. We've got to deal with it and we will."

Frank Koza
Executive Director, Operations Support, PJM Interconnection

"We made the decision [to] harden our backup control system against E1.

[We would now be able to survive an EMP] E1 attack and have a control center that's intact."

John Houston
Senior Vice President, CenterPoint Energy

"NASA… has neither the charter nor the resources to produce and to maintain an actual 24/7 operational space-weather system.

Dr. Daniel Baker
Chairman of the NASA/NAS Space Weather Study

"Three nuclear programs… with a military dimension… If you look at Iran, it's knocking at the door perhaps to get into the nuclear club. North Korea has knocked, is in, and has done three nuclear tests. And the most advanced out of this is Pakistan …"

Dr. Olli Heinonen
Former Deputy Director for Safeguards, IAEA

Crafting an agenda

A number of senior speakers offered strategic perspectives on security concerns, and next steps to enhance resilience and multi-hazard synergy. A common view, emerging from most of the presentations, was that the scale of the risk can only be meaningfully discussed with an assessment of the state of resilience planning and development to address that risk.

The risk associated with severe space weather is high, and operating procedures will likely be insufficient, by themselves, to resolve the problem. And while the impact could be partially mitigated with reliable, early forecasting, that capability does not exist today. As **Dr. Daniel Baker**, Chairman of the NASA/NAS Space Weather Study pointed out, "NASA… has neither the charter nor the resources to produce and to maintain an actual 24/7 operational space-weather system."

Similar concerns were voiced over the risk of malicious EMP, at a time when there has not yet been widespread hardening or planning to address such a threat. **Dr. Olli Heinonen**, former IAEA Deputy Director for Safeguards, pointed to several unstable nations as representing the most serious concern. Iran, he said, is a nation "knocking at the door" to get into the nuclear club, "and North Korea has knocked, is in, and has done three nuclear tests." Pakistan, he said, is the most advanced nuclear weapon country in this class, with the world's fastest growing military arsenal, fifteen years after its first successful nuclear test.

For the Department of Defense, a key area of concern is maintaining the capability of the U.S. military on a Black Sky Day. John Conger, Deputy Under Secretary of Defense in DoD for Installations and Environment, described the problem this way: "The fact of the matter is that on most bases, there's less than a week of gas on those locations. And so if they were cut off, those diesel generators will run out of fuel moderately quickly."

Both natural and malicious hazards are unlikely to resolve on their own, and the focus is increasingly on finding balanced, optimum paths to plan, coordinate and implement cost-effective resilience investments.

Dr. Jane Holl Lute, former U.S. Deputy Secretary of Homeland Security, called for achieving national resilience by working at multiple levels:

(1) Informed individuals
(2) Capable communities
(3) Responsive federal system

When individuals are properly informed, she explained, they are empowered to act, in coordination with community and federal efforts. The federal government has worked to encourage this three-level process, providing grants to communities to help fund local efforts to prepare for such crises.

Dr. Lute called for baseline standards and the use of tools that are already available to dramatically reduce our vulnerabilities. This means we will need to find more people with high-end cyber skills, to confront innovative, persistent adversaries, raising their costs and risks. And as we find them and build more capability in such areas, they will need to be hired, trained and tested to standards. "The status quo should give you no comfort," she told the conference. "The status quo is no pathway to success. The time for complacency is long past us."

Also speaking on the need for standards, Dr. Zvi Rosenstock of Israel's RAFAEL Aerspace Corporation spoke of the need for broadly accepted guidelines for resilience, proposing planning for resilience at a level that would assure limited duration power outages.

For the power industry, achieving resilience will require coordinated action on a large scale. "The last thing we need," said **Nicholas Ingman**, Manager of Operational Excellence for IESO, "is individual areas working in isolation …"

"The status quo should give you no comfort. The status quo is no pathway to success. The time for complacency is long past us."

Dr. Jane Holl Lute
Former Deputy Secretary,
Department of Homeland Security

"The last thing we need is individual areas working in isolation on an issue that covers such a large area. So I really do look to further collaboration and coordination across the industry."

Nicholas Ingman
IESO, Manager of Operational Excellence,
Canada

"I've looked at resilience in corporate America […] We determined that […] the resilient portfolio across all timeframes radically outperformed the non-resilient portfolio."

Jeff Weiss
Managing Director, Distributed Sun

Speakers in this session also talked about government and corporate decision making as a key to any progress in this area. How can decision makers be encouraged to focus on power grid security?

From Israel's Ministry of Home Front Defense, Jacob (Kobi) Wimisberg, Director of the Strategy and Cooperation Division, noted that political leaders will find it easier to support resilience spending if implementation costs can be kept low, and in perspective relative to the risks. The costs of preparing for an EMP strike, he explained, are not high when compared with the likelihood of an attack and the severity of the damage.

Some of the speakers in this session saw management decision-making as the critical first step. **Jeff Weiss**, Managing Director at Distributed Sun, suggested the stock market might prove a useful educational tool to motivate decision makers. Mr. Weiss reported on a research project, showing that resilience-invested companies have typically out-performed competitors in the capital markets, returning to business sooner after a crisis, and their stock prices returned to pre-crisis levels more quickly.

SESSION II

THE ROLE OF GOVERNMENT

Governments at all levels, in coordination with industry,

have a vital role to play in helping plan and prepare power grids for a Black Sky Day. In the United States, some federal and state policymakers have begun taking important legislative and regulatory steps. But a critical missing element, according to **Daniel Poneman**, Acting U.S. Secretary of Energy, has been a holistic approach that cuts across government "stovepipes" to address the threats effectively.

Recognizing the risk

Acting Secretary of Energy Daniel Poneman, the summit keynote speaker, highlighted the critical first step in addressing severe, emerging risks to the national power grid: Recognizing the problem. His remarks were echoed by the full range of U.S. and international speakers, who discussed the many different severe threats our electric system faces in our rapidly changing world.

"National electric grids could be headed for disaster if we don't change our course," said U.S. **Rep. Yvette Clarke**, the Ranking Democrat on the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. "In recent years, rapid technology evolution of national power grids and other vital national infrastructures has substantially increased their vulnerability to serious, widespread damage or disruption by electromagnetic hazards."

Much of the current power grid, Acting Secretary Poneman pointed out, is an anachronism, akin to how we now view typewriters and dial telephones from the early 1970s. It is neither robust nor resilient against some of the most serious emerging threats societies face today. And those threats are multiplying, he added. We face growing cyber vulnerabilities as networks of computers, intelligent electronic devices, software, and communications technologies present greater protection challenges than our traditional infrastructures were designed

"People who are working on energy efficiency over here don't work with the people who are working on storm response over there, who aren't necessarily in the same office that's making the procurements for cybersecurity over here."

Daniel Poneman
Acting Secretary, U.S. Department of Energy

"For the first time since Cold War days, the United States, and its allies have been threatened with nuclear attacks. NASA, the National Academy of Sciences have warned that the Sun around once per century fires a massive coronal mass toward the Earth… Scientists have warned that either one could spell disaster for the electric grid

U.S. Rep. Yvette Clarke
Ranking Democrat, House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"I've spent almost forty years working on nuclear weapons and nonproliferation.

Clearly, although we hope that the odds are very low, that we would be remiss if we did not take appropriate measures.

And I believe […] some of the things we could do to address EMP could help us on GMD, could help us on cyber security, can help us on resilience, can help us on efficiency."

Daniel Poneman
Acting Secretary of Energy

[Speaking of the Congressional EMP Commission's report – ed.]

to handle. And we face electromagnetic threats, from severe space weather and EMP.

Dr. Shlomo Wald, Chief Scientist for Israel's Ministry of Energy and Water Resources, addressed most of his remarks to EMP, which he called "a totally new threat." While the risk is increasingly recognized, it has not yet been addressed by many governments largely, he said, because they assume resilience against a threat of this magnitude would be unaffordable. This, he explained, is a misunderstanding, not least because mitigation actions reduce the probability of an EMP strike.

Also addressing his remarks to EMP, U.S. Rep. **Ed Royce**, Chair of the House Foreign Affairs Committee, described the risk in graphic terms. "If a camouflaged missile with a nuclear warhead is launched from a freighter, and it detonates somewhere over the east coast, the Congressional EMP Commission projected it would mean 70 percent of the U.S. population could be without power for a number of years." Such an attack, he said, could come from a state or a non-state actor.

Failure to recognize and begin preparing for severe threats early could, Rep. Trent Franks explained, lead to unprecedented ethical and legal challenges. If a probable severe hazard is forecast at some point in the future, and the only option for secure protection is to shut down the grid, management could face the risk of causing damage and loss of life, potentially needlessly, to avert a catastrophic hazard.

Given his extensive experience with disaster management, **Richard Reed**, Senior Vice President at American Red Cross and former Assistant to the President of the United States, gave specific examples of the consequences of serious power outages, and the need to work together to mitigate such outages. "How do we mitigate the impacts of what inevitably is going to happen," he asked? "Who knows what the next thing is going to be?"

"I think working together we can come up with some innovative ideas to better manage this," he concluded. "I think if you look at Hurricane Sandy as an example, with all of the herculean efforts from all parts of government, private sector, nonprofit community, we still had a 160-plus deaths from a less than a Category I storm."

"I think working together we can come up with some innovative ideas to better manage this. [For huuicane Sandy] with all of the herculean efforts from all parts of government, private sector, nonprofit community, we still had 160-plus deaths from less than a Category I storm."

Richard Reed
Senior Vice President, American Red Cross,
Former Assistant to the U.S. Presiden

"The EMP problem could even threaten our national continuity. So there is no question we need to take action."

U.S. Rep. Ed Royce
Chairman of the House Foreign Affairs Committee

"We are spreading the word. We are spreading the word internationally. We're beginning to bring resilience to the national grids around the world. And we're making disaster less likely."

The Rt. Hon. James Arbuthnot MP,
Chair, Defence Committee, UK

"We've admired this problem a long time. We have studies to show for that. But I can also see us turning the corner."

William Bryan
Deputy Assistant Secretary, U.S. Department of Energy

Making progress

Increasingly, resilience of critical infrastructures to serious, large scale threats is seen as a vital national priority. For the U.S. and some of its key allies, progress is being made in addressing such vulnerabilities.

Over the last year, government agencies have begun focusing increasing attention on planning for power grid resilience as a priority for security and continuity. To ensure plans are connected to realistic budget projections, there has been particular interest in investments that address multiple hazards.

Secretary **Daniel Poneman** expressed this approach succinctly: "The same investments in many cases that can help prevent disruptions during any one of these disasters can lead to a more resilient grid against all of these disasters – hurricanes, tornadoes, floods, nuclear attacks, cyber attacks, solar events. We can all agree the need for action is clear."

William Bryan, DOE Deputy Assistant Secretary, also referred to the need for action, highlighting some recent steps. "We've admired this problem a long time. We have studies to show for that. But I can also see us turning the corner." He noted a resurgence in U.S. manufacturing capacity for large-scale transformers, and spoke about the Sunburst Sensor Program, a DOE / EPRI partnership working to help measure Space Weather-induced currents and impacts.

Also in the United States, regulators are beginning to prioritize resilience measures to protect critical assets against severe, wide area risks. The U.S. Federal Energy Regulatory Commission (FERC) took landmark action in late 2012, finalized in May, 2013 shortly before the summit, that will mandate grid protection measures against severe space weather. "Now," FERC Commissioner **Cheryl LaFleur** said, "all the smart folks in industry… have to sit down and come to consensus on this" and "vote in a standard and submit it within the timeline for us to then act on and for it to become the force of law."

Steps are also being taken by regional and local government bodies. In Maine, for example, with leadership from State Rep. Andrea Boland, the power industry, public utilities commission and legislature are working to set priorities and timelines to address power grid vulnerabilities to electromagnetic threats.

Several U.S. allies have taken independent steps to protect their power grids against electromagnetic threats and other severe hazards. Israel, in particular, is working to enhance power grid protection at the same time the nation is taking steps toward transitioning from one electric company, Israel Electric Company to independent power producers.

As one of its approaches to power grid resilience, Israel invests in redundancy in both its generation and transmission networks, along with assigning a high priority to training and emergency exercises. These measures worked well over the last two years, for instance, when Israel successfully operated through an unplanned natural gas shortage.

"My focus has been moving from studying the effects of geomagnetic disturbances on the grid to taking action [...] to protect the electric grid. I am happy to report that I think we took a major step toward that goal… with FERC's final rule on reliability standards for geomagnetic disturbances."

Cheryl LaFleur
Commissioner, U.S. Federal Energy Regulatory Commission

"And one thing I've learned [...] is that it is cheaper and more effective to deal with these problems up front by the investments you make on the front end than to have to deal with the damages and the consequences after some horrible event should occur."

Daniel Poneman
Acting Secretary, U.S. Department of Energy

"We have to think beyond merely restoration, to building a better, safer, stronger, more resilient grid. And, yes, one that can be resistant to electromagnetic pulse, geomagnetic disturbances, and the like."

Daniel Poneman
Acting Secretary of Energy

Crafting an agenda

With government focus on power grid resilience growing and initial steps being taken, government representatives at the summit offered their perspectives on some of the best approaches needed to guide next steps, as well as some of the key principles motivating such effort.

Looking to the future, Acting Secretary Poneman proposed setting the bar high as we look to enhance grid resilience. "We have to think beyond merely restoration, to building a better, safer, stronger, more resilient grid. And, yes, one that can be resistant to electromagnetic pulse, geomagnetic disturbances, and the like." He also called for taking a "holistic" approach, finding ways to bridge the "stovepipes" of separate government bodies. "That," he said, "will enable us to see that some of the things we could do to address EMP could help us on GMD, and that could help us on cyber security, and that could help us on resilience, and that could help us on efficiency." And since government doesn't have all the assets, resources or answers, he said, all the relevant parties, public and private, must work together: federal, state and local executive and legislative bodies, and both public and private industry.

Andrew Miller MP, who chairs the U.K. Science and Technology Committee, expanded this list further, pointing to the need to bring scientists and engineers together with government bodies, to help them understand the risks of hazards like severe space weather, and the options for resilience.

U.S. Reps. Trent Franks and Yvette Clarke spoke of the need for a national standard to protect the grid against electromagnetic hazards, pointing to the SHIELD Act as an example of legislation that could mandate such a standard, calling for industry, rather than government, to craft the standard.

Israel's Energy Ministry Chief Scientist Dr. Shlomo Wald called for a wide range of public and private steps to build resilience against the risk of an Electromagnetic Pulse. EMP is "a totally new threat," he said. And since it could become an existential threat that could cross national boundaries, he called for international collaboration – developing common standards, methodology and approaches to cross-sector response and

"The same investments in many cases that can help prevent disruptions during any one of these disasters can lead to a more resilient grid against all of these disasters – hurricanes, tornadoes, floods, nuclear attacks, cyber attacks, solar events… "

Daniel Poneman
Acting Secretary of Energy

"If we harden the power grid to minimize the fallout from an EMP attack, it reduces the incentive frankly for our enemies to attack us. And that's ultimately what we want to do."

U.S. Rep. Ed Royce
Chairman of the House Foreign Affairs Committee

"People are talking about […] how to control and manage the disaster. I'm afraid in [the] case of EMP, all the command chain will collapse."

Dr. Shlomo Wald
Chief Scientist, Israel Ministry of Energy and Water Resources

recovery. In looking toward appropriate standards, he echoed the comments of many other speakers: "We shouldn't look for continuous operation of the grid," he said, but rather "affordable shutdown." If the requirement for mitigating a severe event like EMP is changed from continuous operation to reasonable recovery time, he said, you build resilience while reducing the required investment by an order of magnitude.

Looking forward, **Shlomo Wald** called for requiring the private sector to take steps to mitigate an EMP attack, focusing on other critical industries beyond electric companies, including critical financial and security databases. He also suggested, in the long term, looking at distributed micro-grid architectures that could help enhance resilience against such hazards. A more resilient grid, he added, will protect against not just EMP events but also cyber and many other threats.

SESSION III

THE ROLE OF INDUSTRY

With power grids in modern countries largely owned and controlled by private industry, private sector input, initiatives and collaboration with other societal stakeholders will be critical for any successful strategy to protect against Black Sky Day hazards.

Leaders in the electric industry have increasingly recognized their responsibility to address such hazards.

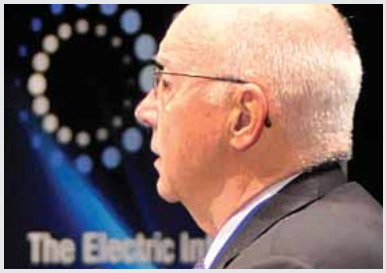
As a trans-national global industry focused on projecting and addressing emerging risks, the insurance industry also has an important role to play, and insurance companies have become important participants in the evolving dialogue on power grid resilience to severe hazards.

"There's a convergence of both infrastructure technologies and attack technologies […that] moves the puck sooner than we all expect."

Joe McClelland
Director, Office of Energy Infrastructure Security, FERC

Recognizing threats

One of the common themes expressed in this session was the challenging and disturbing correspondence between rapid development of high performance, highly leveraging societal infrastructures and technologies, and rapid growth of hazards that threaten them. Where such infrastructures, like the power grid, become essential to society, this convergence becomes an existential threat.



"All of this enhancement has come at the cost of a vulnerability, […] an enormous vulnerability to solar weather and to the human hostility component that we cannot seem to remove from the human genome."

Richard Murray
Head, Liability Subcommittee, Climate Risk and Insurance Initiative. The Geneva Association

"There is a perversity in the human-development cycle," **Richard Murray**, Chief Executive Officer of Liability Dynamics Consulting, LLC, said of the growing threats to the power grid, "that has never been more evident than it is today.

"The advances in our lifetimes," he explained, "in technology, telecommunications, and satellite-positioning activity, are enormous and totally unforeseeable. [...] But, all of this enhancement has come at the cost of a vulnerability, […] an enormous vulnerability to solar weather and to the human hostility component that we cannot seem to remove from the human genome." Referring to risks associated with a

"I've heard a sense of urgency today in everyone that we've heard from, but I think the worst possible approach we could take is to just say this is too big, it's too much, we can't possibly do it."

"There's a lot of steps to solving this. […] But to think it's just too big so we have to just keep talking about it for another five years is clearly not the way to go."

Joe McClelland
Director, Office of Energy Infrastructure Security, FERC

predicted Carrington Event – a repeat of a severe space weather event that caused serious damage to the limited electric infrastructures in-place when it last occurred in 1859 – he spoke of the potential for societal damage measured in trillions of dollars.

His warning was echoed by Neil Smith, Manager of Emerging Risk and Research for Lloyd's, who summarized Lloyd's-commissioned research pointing to a "cascade of operational failures" that could put tens of millions of households at risk of power outages lasting from weeks to years.

Joe McClelland, Director of FERC's Office of Energy Infrastructure Security, also echoed the point, saying, "There's a convergence of both infrastructure technologies and attack technologies. The emergence of automation with weapons development…," he said, "moves the puck sooner than we all expect." He pointed to new vulnerabilities anticipated with the expected doubling of smart meters in-use by 2015, to the potential for increased transformer GIC vulnerability as efficiencies continue to rise, and to rapidly accelerating international development of small, short range non-nuclear EMP (IEMI) weapons.

The Rt. Honorable James Arbuthnot MP, Chair of the Defence Select Committee in the U.K. House of Commons, said the EMP threat is growing. North Korea and Iran, for example, have apparently practiced missile launches consistent with an EMP attack. Today, any nation with EMP or IEMI capability already has the power to shut down portions of another nation's critical infrastructure, he pointed out. In the years to come, he forecast, non-state actors or even individuals will be able to do the same thing.

Arbuthnot was joined by Dr. Shlomo Wald, however, in a warning. As an emerging threat, and with the potential for damage on unprecedented scales, it is often difficult for decision makers to grasp both the scope of the risk, and the potential for mitigation. Both speakers said that nations need, and do not yet have, a clear understanding and policy addressing the threat.

Making progress

With more than 3000 power companies in the United States alone, most of the challenge to building resilience to emerging Black Sky Day hazards remains in the future. However, there are important examples of corporations working to address these concerns in the power industry, and increasing awareness and interest in the global insurance sector.

CenterPoint Energy has been working with Siemens PTC to develop designs for GIC-resistant EHV transformers, according to its Senior Vice President John Houston. The company has also been working as a partner with the Department of Homeland Security and the Department of Energy on a rapidly deployable spare transformer program.

Gerry Cauley, CEO and President of NERC, spoke about progress being made in industry, and the range of options ahead. "The value of this summit," he said, "is exploring an emerging challenge and seeing the diversity of perspectives." He also pointed to opportunities to go forward, and take action. As an example, he noted that some power companies are looking at a variety of ways to protect their systems against natural or man-made attacks. Including testing blocking devices.

One of the important messages from the summit was the importance of cross-sector dialogue, in helping to address concerns that could dramatically affect societal health and security. "We believe it's absolutely crucial for the insurance industry to engage with the energy industry and government to tackle this problem," said Neil Smith (Lloyd's).

And for at least some Black Sky Day hazards, "we're seeing increasing awareness now," said Paul O'Neill, the Global Head of Energy at Allianz AGSC. "There's an example in Saudi Aramco where 30,000 PCs were impacted by a virus, and they – as all companies now are – started to ask us for feedback on what we're seeing as best practices on a global basis."

"I do see a lot of common ground. I do see action, and I see some areas of common concern that can serve as the basis for action going forward."

Gerry Cauley
President and CEO of NERC

"We believe that the electrical power systems and grids are particularly vulnerable to solar storms. […] Loss of power could lead to a cascade of operational failures that could leave society and the global economy severely disrupted."

Neil Smith
Manager, Emerging Risk and Research, Lloyd's

"There is no reason that we shouldn't be able to resolve the solar vulnerability to every utility in the United States."

John Houston,
Senior Vice President,
CenterPoint Energy

"When we deal with extreme events that do not respect borders [...] there is a capacity of insurance to work with multiple governments ..."

Richard Murray
CEO, Liability Dynamics Consulting, LLC

Crafting an agenda

Although both public and private sectors have important stakes in resilient infrastructures, the (mostly private) energy sector will be the most important factor in achieving a Black Sky Day – resilient grid. Summit speakers broadly concurred that coordinated, comprehensive planning will be required, along with investments in equipment, procedures and training. But getting to that point will require development of new initiatives and tools by, and for, private and public power companies.

"The real challenge I think we're facing is that as a culture, as a government, as a civilization: we are very good at learning from experience," said Avi Schnurr, CEO and President of the Electric Infrastructure Security Council. What's wrong with this approach? "The problem is when […] the forecast, the level of that problem is so severe potentially that you really don't *want* to learn from experience." Even a single experience of such a threat could be shattering for society. In that case, he pointed out, "you must invest in resilience. That's an area we're not so good at."

Recent history proves the point. Congresswoman Yvette Clarke represents a House district in Brooklyn, NY. As she put it, "We never thought that a super storm like Sandy would hit New York City, but it did. And what is even more interesting is that, for years, they had been modeling out in the public domain of what would happen to New York City if such a storm would hit. And many saw it as just science fiction… Our task," she added, "is to move this discussion out of the realm of science fiction and into reality."

James Arbuthnot MP called for considering a broad agenda: public education, commercial incentives for industry and government measures, with several goals in mind – hardened infrastructure, new protocols and policies, and exercises to tests those protocols and policies. All of those improvements, he added, should be shared internationally so that we have "common standards" around the world.

Insurance industry officials foresee an important role for their corporate sector. "When we deal with extreme events that

do not respect borders when something goes wrong," said **Richard Murray** from Liability Dynamics Consulting, LLC, "insurance is in a very good position to respond without regard to borders in trying to put things right as quickly as we can. Whether it is in preemptive resilience or in mitigation steps afterwards, there is a capacity of insurance to work with multiple governments that is not present in any other resource that we're aware of." And the insurance industry, Murray continued, can help quantify the potential damage of an attack on the power grid, which would help motivate key parties to take steps to reduce the size of potential losses.

How serious is the risk? "We believe that the electrical power systems and grids are particularly vulnerable to solar storms," said Neil Smith, Manager of Emerging Risk and Research for Lloyd's. "A major event could present a systemic risk. For example loss of power could lead to a cascade of operational failures that could leave society and the global economy severely disrupted."

Paul O'Neill, Global Head of Energy, Allianz AGSC, told the summit delegates that the insurance industry is in a unique position to encourage development of best practices. "There is real opportunity to spread best practices to ensure for the common good that we identify these risks, evaluate them, and then reduce the possibility of the outcome and consequences. **Robert "Buddy" Dobbins**, a Technology Director for Zurich North America, concurred, adding that such best practice development could range from protective hardware to operational procedures.

"What will happen now if the Carrington Event repeats itself over Europe, Russia, North America?

We believe our electrical equipment is vulnerable […] So here's my question. If we know that there's a risk, and we suspect how large the exposure can be, and we know there are ways to actually mitigate or possibly even prevent the damage from occurring …, what have we been waiting for?"

Robert "Buddy" Dobbins
Technology Director, Machinery Breakdown, Zurich North America

The Path Forward

In the final segment of the summit plenary session, speakers offered summary comments and perspectives on where industry, government and other stakeholders need to go from here.

What should be done, and how important is it that we find a way to get it done?

Some of the industry representatives present introduced a note of optimism. "There is no reason that we shouldn't be able to resolve the solar vulnerability to every utility in the United States," said John Houston, Senior Vice President at CenterPoint Energy. "And I think that's well on the way." And Avi Schnurr, EIS Council President and CEO, acknowledged there are signs of progress. "I think we're in a very good place this year as opposed to where we've been in previous years," remarked Avi Schnurr, EIS Council President and CEO.

However, the primary message from government representatives was sobering. With bipartisan representation from both the U.S. Congress and the U.K Parliament and administration representatives from Israel, a clear message was articulated: As Representaitve Yvette Clarke (D, NY) put it:

"I do not want any community to be caught off guard by an EMP and geomagnetic disturbances to the grid. And so our job, our task is to move this discussion out of the realm of science fiction into reality."

How can this be accomplished? Communication and education are essential, for the public, for industry and for government.

"We politicians are merely a reflection of the people we represent," said **Andrew Miller** MP, Chair of the UK Science and Technology Committee. "We need to strengthen that bridge between science and policymakers at all levels of the political process."

Dr. **Shlomo Wald**, Chief Scientist of Israel's Ministry of Energy and Water Resources, agreed that communication and education are essential. While warning that this will be a challenge, he suggested, in regard to EMP protection, that goal should be a clear understanding of the urgency, leading to development of clear, internationally coordinated policies.

"Risk can be very much reduced if we prepare ourselves properly ahead of time, before the disaster."

Dr. Shlomo Wald
Chief Scientist, Israel
Ministry of nfrastructures and Energy and Water Resources

"We need to strengthen that bridge between science and policymakers at all levels of the political process."

Andrew Miller
MP, Chair, UK Science and Technology Committee

If this is important to you ... get involved."

Avi Schnurr
CEO and President, EIS Council

"We have a lot of work to do. Off we go."

Rt. Hon. James Arbuthnot MP

These comments resonated with a warning offered earlier in the summit by Acting Energy Secretary Daniel Poneman. Just hoping for the best, he implied, would be a serious mistake.

“When you think back on recent history, those things that have completely disrupted our lives, in many cases, were the last thing any of us would've ever expected.”

Where do we go from here? According to **Avi Schnurr**, EIS Council President and CEO, there are many opportunities to get involved.

“Whereas a few years ago the question was: ‘Would anything happen, would anything go forward,’ we're no longer dealing with that… If you have ideas, if this is important to you because you are a stakeholder in the energy industry, the insurance industry, the government, or simply as a private citizen, there are now several dimensions and opportunities to get involved.”

EIS Summit (EISS) is hosted as a government / NGO partnership. EISS NGO Hosts:

EIS COUNCIL

www.eiscouncil.org

THE HENRY JACKSON SOCIETY

DEMOCRACY · FREEDOM · HUMAN RIGHTS

www.henryjacksonsociety.org