THE FIFTH ANNUAL WORLD SUMMIT ON INFRASTRUCTURE SECURITY
Electric Infrastructure Security Summit V
United Kingdom

The fifth 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 V moved from assessments of current status to recommendations for next steps that could enhance grid resilience against multiple hazards.
Electric Infrastructure Security Summit V
Summit Report

Published:
July 20, 2015

Edited by:
Avi Schnurr
EISS Series Coordinator
CEO and President, EIS Council

Note on text formatting: Where quotes are emphasized as “pull-quotes” in parallel with the text of the report, editing marks have been removed and slight adjustments have sometimes been made to meet the graphic requirements of the report, and to simplify reading. In all such cases, the original quote, with editing marks, may be found in the report text.
Overview

"Assessing resilience for wide-area grid outages from E-threats and other hazards"

There is broad agreement on the importance of resilience investment and restoration planning to assure grid continuity regarding “black sky days”: extraordinary and hazardous catastrophes utterly unlike the blue sky days during which utilities optimally operate.

EISS V focused on this objective. Summit sessions examined the hazards, considered policy implications, and reviewed today’s status and the enhanced resilience and response planning now beginning to take place in both public and private sectors.

**EIS SUMMIT SERIES ORGANIZING COCHAIRS**


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 V, LONDON**

**Government and Organizations**

United States Department of Energy, North American Electric Reliability Corporation

**Individuals and Foundations**

Table of Contents

Executive Summary ........................................................................................................................................... 11

Session One | Severe Hazard Review and Update .......................................................................................... 15

Session Chair: The Rt. Hon. James Arbuthnot MP, United Kingdom .................................................... 17
Keynote Address: "Energy Security": Suzanne Spaulding, Undersecretary for National Protection and Programs Directorate, DHS .................................................................................................................. 18

Panel 1 | Natural Hazard Review: Severe Space Weather, Large Regional Earthquake ........................... 21
Dr. Daniel N. Baker, Chair, NASA/National Academy of Sciences Severe Space Weather Study .......... 22
William Murtagh, Program Director, NOAA Space Weather Prediction Center .................................. 23
John Kappenman, Principal Investigator, National Academy of Sciences
Severe Space Weather Project ......................................................................................................................... 24
Jonathon E. Monken, Director, Illinois Emergency Management Agency (IEMA); Chairman, Central United States Earthquake Consortium (CUSEC) .................................................................................................................. 25

Panel 2 | Security Briefings: Manmade Hazards
Part One: Cyber Terrorism: Considering a Sophisticated, Coordinated Threat .................................... 29
Gerry Cauley, CEO and President, North American Electrical Reliability Corporation ............................ 30
David Croom-Johnson, Underwriter, Aegis Insurance Services, Inc. ......................................................... 31

Part Two: Catastrophic Coincidence: Conventional or Non-Conventional and Malicious Hazards .................................................................................................................................................................................. 33
Dr. Paul Stockton, Former U.S. Assistant Secretary of Defense ............................................................... 34

Part Three: E-threats: EMP, IEMI ................................................................................................................. 37
Dr. Ollie Heinonen, Former Deputy Director General for Safeguards, IAEA ......................................... 38

Session Two | Status: Where Are We Today? ................................................................................................ 41
Session Chair: Mr. Trent Franks, Representative, U.S. Congress, House Armed Services Committee 43

Panel 1 | Corporate Energy Sector - Accomplishments and Work In-Progress ..................................... 41
Dr. Chris Beck, Vice President for Policy and Strategic Initiatives, EIS Council ..................................... 46
Dr. David Elmakis, Senior Vice President, Planning, Development & Technology,
Israel Electric Corporation ................................................................................................................................. 47
Jarmo Elovaara, Fingrid Oyj ......................................................................................................................... 48
Chris Train, Director, Network Operations; Group Director for Safety, Sustainability, and Resilience at National Grid UK National Grid ................................................................................................................. 49
Thomas J. Galloway, President and CEO, North American Transmission Forum ................................. 51
Panel 2 | Government Sector: International, National, Regional .......................... 53

Joseph McClelland, Director, FERC, Office of Energy Infrastructure Security ........................................ 54
William Bryan, Deputy Assistant Secretary, U.S. Department of Energy ........................................... 56
Dr. Shlomo Wald, Chief Scientist, Israel Ministry of Infrastructures, Energy and Water Resources ... 57
Roger Steen, Team Supervisor, Contingency Planning & Crisis Management, Norwegian Water Resources and Energy Directorate (NVE) ............................................ 58

Panel 3 | Life-Sustaining-Critical Infrastructures and Other Sector Perspectives ............. 61

Miles Keogh, Director of Grants and Research, National Regulatory Commissioners Association (NARUC) .......................................................... 62
Kelly Speakes-Backman, Commissioner, Maryland Public Service Commission .................. 63

Session Three | Policy Implications ................................................................. 67

Keynote Speakers .................................................................................................................. 69

Caitlin Durkovich, Assistant Secretary for Infrastructure Protection, Department of Homeland Security, U.S. .............................................................. 70
Cheryl Lafleur, Acting Chairman, Federal Energy Regulatory Commission, U.S. .................. 73

Panel 1 | Government Perspectives ................................................................. 77

Andrew Miller, MP, Chair, Science and Technology Committee, UK ........................................... 78
Dr. Peter Pry, Former Chief of Staff, U.S. Congress EMP Commission; CEO, Taskforce on National and Homeland Security ......................................................... 79
Todd Rosenblum, U.S. Acting Assistant Secretary for Defense for Homeland Defense & Americas’ Security Affairs ......................................................... 80
Dr. Dan Weinstock, Former Director, Electricity Authority, Minister of National Infrastructures, Israel ... 81

Panel 2 | Corporate Perspectives ................................................................. 83

Terry Boston, CEO, PJM Interconnection .......................................................... 85
Dr. Sanjay Bose, Vice President, Central Engineering, Consolidated Edison ......................... 87
Gerry Cauley, CEO and President, NERC ................................................. 89
John Houston, Division Senior Vice President, High Voltage Delivery and Compliance, CenterPoint Energy ..................................................................................... 90
Robin Manning, Executive Vice President, Tennessee Valley Authority ......................... 92
David K. Owens, Executive Vice President, Business Operations, EEI ................................. 94

Session Four | Multi-Sector Planning for Black Sky Days ........................................ 99

Introduction .................................................................................................................. 101

Dr. Paul Stockton, former U.S. Assistant Secretary of Defense, Editor-in-Chief, EPRO Electric Infrastructure Protection Handbook ......................................................... 102
Panel 1 | Electric Sector ...........................................................................................................107

Dr. David Elmakis, Senior Vice President, Planning, Development & Technology,
Israel Electric Corporation ................................................................. 108

Gerry Cauley, CEO and President, NERC ......................................................... 109

Dr. Trevor Gaunt, Professor, Department. Of Electrical Engineering,
University of Capetown, South Africa ................................................. 111

Frank Koza, Director of Operations, PJM ................................................. 113

Raj Rana, Former Director - RTO Policy and NERC Compliance, AEP ... 114

Panel 2 | Regional and Local Government ..............................................................................117

Miles Keogh, Director of Grants and Research, National Regulatory Commissioners
Association, (NARUC) ........................................................................ 118

Thomas MacLellan, Director, Homeland Security & Public Safety Division,
National Governors’ Association .......................................................... 120

Jonathon E. Monken, Director of Illinois Emergency Management Agency (IEMA);
Chairman, Central United States Earthquake Consortium (CUSEC) .......... 122

Panel 3 | National and Federal Government ...........................................................................127

Caitlin Durkovich, Assistant Secretary for Infrastructure Protection,
Department of Homeland Security, U.S. .............................................. 128

William Bryan, U.S. Deputy Assistant Secretary of Energy ....................... 129

Todd Rosenblum, U.S. Acting Assistant Secretary of Defense for Homeland
Defense & Americas’ Security Affairs .................................................. 130

Joseph Shapiro, Director of Threat Scenarios Department, Ministry of Home Front Defense, Israel 132

Panel 4 | Non-Government Organizations - Emergency Community Support ....................135

BGen (ret.) Meir Elron, Director, Homeland Security Program, Institute for National Security
Studies, Israel ...................................................................................... 136

Eddie Blackmon, Southern Baptist Disaster Relief (SBDR), North American Mission Board SBDR
Coordinator ...................................................................................... 138

Avi Schnurr, CEO and president, EIS Council .......................................... 140

Conclusion | Where Do We Go From Here? ...................................................................145

The Rt. Hon. James Arbuthnot, MP ............................................................. 147

Terry Boston, CEO, PJM Interconnection .................................................. 148

Dr. Shlomo Wald, Chief Scientist, Israel Ministry of Infrastructures, Energy and Water Resources ... 150

William Bryan, U.S. Deputy Assistant Secretary of Energy ....................... 152

Joseph McClelland, Director, FERC Office of Energy Infrastructure Security .................................. 153
Executive Summary
Executive Summary

As the fifth annual world summit on infrastructure security, EISS V provided a unique, comprehensive look into emerging “Black Sky Hazards”: Severe threats to the power grid and other lifeline infrastructures. Beginning with security briefings and other updates on these hazards, senior government managers, industry and NGO executives, scientists and invited delegates from more than twenty nations spent two days in discussions focusing on action-oriented opportunities for progress in addressing this issue.

The discussions were focused through presentations and discussions addressing questions associated with these infrastructure security concerns. What is our best understanding of these threats today? Where are we – government, industry and NGOs – in preparing resilience and response measures to address them? And finally, what opportunities can be identified for incremental progress, both in addressing the hazards directly, and in looking for ways to enhance “whole of nation” response? What improvements can be recommended, building on existing government and industry disaster management structures, to better address these emerging hazards?

Many recommendations and conclusions emerged, including fundamental suggestions to enhance resilience to severe power outages. Two examples:

- **Power grid protection measures for electromagnetic threats.** EMP and Severe Space Weather protection measures should be tiered, applied for selected hardware “enclaves” as a basis for power restoration, and supplemented by staged spares, identified in an updated, widely accessible inventory. Regulatory rulings, where they apply, typically provide a foundation for such measures, to be supplemented by best practices where required for critical hardware.

- **Power grid restoration from any black sky hazard.** Restoration from a wide regional, long duration outage from any severe hazard will require support from industry’s partners, including government agencies and mass care NGOs. Power restoration support should be a priority for whole community response, with existing emergency coordination structures expanded to include comprehensive, cross-sector participation, with a well-defined, operational leadership process. As one senior electric sector leader commented, recalling previous power outages like Superstorm Sandy, “It was very chaotic. Nobody was in charge.”

The summit included, for the first time, extensive discussion of the first volume of the **Electric Infrastructure Protection Handbook**, focused on expanding guidance already provided for Handbook development by industry, government and NGO stakeholders.

Based on the presentations and discussion, the formation of a new **EPRO Executive Steering Committee** was announced as a companion project to the Handbook. **EPRO ESC**, to be chaired by Terry Boston, CEO and President of PJM and coordinated by Dr. Paul Stockton, is designed to help facilitate cross-sector connectivity and coordination of industry and government agencies, as they build expanding capabilities to address black sky hazards.
Session One

Severe Hazard Review and Update
In his introductory remarks, James Arbuthnot began by referring to growing concerns over emerging, severe threats to critical infrastructure. Such concerns, he pointed out, are now shared by officials at the highest levels of government.

"[What was] the answer the British Prime Minister gave in January, when he was asked by the Chairman of the Joint Committee on the National Security Strategy: ‘With hindsight, Prime Minister, is there anything you think the National Security Council has missed?’"

"I’m not a scientist with knowledge of EMPs, and space weather. It would have been useful to have been able to get politicians to challenge the officials and the machinery with questions like, “Have we got this covered…?”

As our dependence on organic, interdependent infrastructures grows, societies face growing risk from both emerging hazards like e-threats, and the full range of other severe “black sky” hazards. With these growing concerns, the EIS Summit series, he explained, has broadened its focus to include the full set of such severe hazards.

“Cyber, EMP, space weather, severe earthquake, severe terrestrial weather. All of which are capable of causing real widespread blackouts due to damage and disruption to power grids and other utilities.”

Most countries are not well prepared, he pointed out, for the complex planning needed to mitigate such hazards. In that regard, James Arbuthnot announced the new Electric Infrastructure Protection Handbook, due to be published later in the year.

Edited by former U.S. Assistant Secretary of Defense Dr. Paul Stockton, the EPRO Handbook "brings together ideas from previous summits and seminars, [with] contributions from national and regional governments, emergency response organizations, and the power industry.” As a new, first of its kind resource addressing cross-sector resilience approaches for severe hazards, the draft Handbook would be used to help frame the discussions – and solicit delegate input – for Day Two of the summit.

---

1 James Arbuthnot retired from Parliament in 2015
Keynote Address: "Energy Security"

Suzanne Spaulding, Undersecretary for National Protection and Programs Directorate, DHS

In her keynote address, Undersecretary Spaulding focused on the need for broad partnerships to achieve effective resilience for severe infrastructure hazards.

“Our overarching mission,” she said, “is to strengthen the security and resilience of our nation, the United States’ critical infrastructure. But we are very aware that we … do this in a global context.”

In particular, effective strategies for national security and resilience must include all hazards, and must connect all relevant societal sectors.

“An all-hazards approach and a cross-sector approach,” she pointed out, “[is] one of the things that Department of Homeland Security brings to this effort … to help bridge the efforts of the various critical infrastructure sectors.”

As an example, she said, “A particular focus these days on making sure that we are coordinated in our response activities.”

Part of this holistic approach, of course, is to ensure all critical infrastructures – and all relevant sectors – are brought together. Thus, the definition of critical infrastructure must, itself, be quite broad.

“Our definition of critical infrastructure is … those assets, systems, and networks, physical or virtual, so vital that their disruption would have a debilitating impact on national security, economic security, or public health and safety or any combination therein.” And given this breadth of critical infrastructures, it also becomes clear that disruption of these interdependent systems can come from a wide variety of threats.

“... Our focus at the Department these days is on bringing greater unity of effort.

“... Everybody [needs to] understand what everybody else has and can bring to the table. And then you’ve got to have really good communication during an event.
Given the combination of a wide range of critical infrastructures, and a growing set of severe hazards, resilience planning cannot be static. “This area is so dynamic, the context is so fluid. I think we have to think in terms of comparative advantage. And the only way you can really effectively bring comparative advantage to the table is if everybody understands what everybody else has and can bring to the table. And then you’ve got to have really good communication during an event.”

Given the centrality of energy to all critical infrastructures, DHS works closely with the Department of Energy. “Our whole of government approach … means that we work very closely with the Department of Energy … the sector specific agency with the lead for the energy sector.” In addition, “across the critical infrastructures, that whole government approach [means] we work closely with our law-enforcement and intelligence colleagues. Only by bringing all of that together can we meet this challenge.”

This “whole of government” [approach] goes far beyond federal agencies. “Whole of government also means the states, localities, the territories and the tribes, the SLTTs. And Caitlin [Assistant Secretary Caitlin Durkovich -- ed.] is particularly effective at making sure that we’re reaching out and bringing those important partners in both as owners of critical infrastructure, and as part of the security solution.”

And the private sector is central to this partnering process. “A ‘whole of nation’ approach means we’ve got to go beyond government … we’ve got to view the private sector, owners, particularly those critical infrastructure owners and operators as true partners … in achieving the security and resilience that we need.”

In summary, the Undersecretary made it clear that there is a growing sense for the need to address our increasingly interdependent critical infrastructures with a corresponding approach to help assure connectivity among all resilience stakeholders: the “whole of nation” approach.

“This is way beyond the Department of Homeland Security. It is beyond what the government itself can do. It is beyond what the private sector can do. It is beyond what the United States can do on its own. It really does take the kind of collaboration that I know will take place … in this room over the next two days.”
Dr. Daniel Baker, William Murtagh, John Kappenman and Jonathon Monken provided an update on several black sky hazards. GMD was discussed in the context of relatively recent solar activity, with a severe coronal mass ejection missing earth-impact in 2012 by about one week in the earth’s orbital position around the sun. And panelists warned that national power grids, in general are becoming more sensitive to these events.

There is good news on international cooperation: The U.K. and the U.S. are now beginning 24/7 information sharing on solar weather.

Severe, regional earthquakes were discussed from the perspective of the recent Capstone 14 exercise, which focused on an earthquake in the New Madrid Seismic Zone. Key lessons learned from that exercise include the importance of gasoline, as a critical resource for many life saving, life sustaining missions. However, there is no national strategy today to ensure emergency power resources or fuel distribution are available for critical assets.

Concerns were also raised that additional analysis is needed to look at potentially critical indirect impacts of a New Madrid earthquake, with the nation’s primary natural gas and crude oil pipelines running through the fault zone.
Dr. Daniel N. Baker, Chair, NASA/National Academy of Sciences
Severe Space Weather Study

Dr. Baker reviewed the work of the NASA/NAE team. At the time, he explained, “we were asking the question how severe can storms become.” Since the report, their conclusions were validated by observations. As an example, his presentation included images of a coronal mass ejection that occurred in July, 2012.

In an event comparable in size to the now-famous Carrington Event, which caused serious disruptions even to the primitive telegraph system of the time, “This blast of material came out from the sun at about 3,500 kilometers a second. It moved out from the sun to the earth’s orbit in about eighteen hours.”

With measurements for the event from sensors on spacecraft, they were able to model what would have happened if the CME had encountered the earth. “Had this event occurred about a week earlier or so, it would have been a direct hit on the earth, and this would have been I think devastating in its consequences … We’d still be picking up the pieces.”

In summary, he said, “we don’t have to look back to the musty old records. In the midst of what most regard as a fairly modest solar activity period … the sun was able to generate an immensely powerful event.”

“Had this July, 2012 solar CME event occurred about a week earlier or so, it would have been a direct hit on the earth with devastating consequences.

“We would still be picking up the pieces.”
Bill Murtagh expanded further on the subject. Referring to a tendency to assume that major solar events are closely associated with intense solar cycles, he pointed to the 23rd of July 2012 CME as a very recent counterexample. “Big events do occur with small solar cycles … the event that occurred on the 23rd of July that Daniel just talked about is a great example. … We were lucky, it just wasn’t earth-directed.”

In addition, he said, “these big space-weather events can occur at any stage of the solar cycle, so let’s not get hung up on the solar maximum.”

Bill Murtagh also spoke of new initiatives moving forward in NOAA, to help address concerns with severe space weather. “One of the key things, and I’m very pleased to announce this, is the Discover spacecraft is due to be launched in … January of 2015. … We’ll have our sentinel in space.”

NOAA is also working with colleagues in the U.S. and worldwide “on a modeling capability that will help us understand everything from what’s happening in the sun and how it transitions to here on earth [to] how the earth reacts.”

And finally, he referred to the new partnership between the U.S. and the U.K. on solar weather. “Another exciting initiative is our partnership, indeed, with the United Kingdom … on the 8th of October this year will [initiate] 24/7 operations …with their Space Weather Operations Centre.”

“Big events do occur with small solar cycles. The event that occurred on the 23rd of July is a great example. We were lucky, it just wasn’t earth-directed.”

“I’m very pleased to announce that the Discover spacecraft is due to be launched in January of 2015. We will have our sentinel in space.”

“On the 8th of October this year, our partnership with the United Kingdom will initiate 24/7 operations, with their Space Weather Operations Centre.”
John Kappenman, Principal Investigator, National Academy of Sciences Severe Space Weather Project

John Kappenman joined his colleagues on the panel in expressing concern for the potential disruption that could be caused by severe space weather. Tempering this concern somewhat, he began his remarks by referring to progress that has been made. “We’ve seen a lot of progress, especially in the public policy arena in regards to geomagnetic disturbances, … with efforts underway to develop standards. In this regard, the Federal Energy Regulatory Commission has directed the industry through NERC to propose some standards for this important topic.”

Such efforts are timely, he explained, due to increasing vulnerability of the U.S. power grid. However, he voiced his concern that standards developed fully address grid vulnerabilities.

“We’ve been in a trend line for many decades, of increasing vulnerability of the US power grid infrastructure to this particular threat.”

Thus, he said, it is important to ensure that any benchmark threat accurately reflect the potential for a severe CME. “There was an event, for example, in 1982 where as much as near 2,700 nanotesla per minute was actually observed. [And] we know of an event that occurred in the March 1989 storm where we actually measured at the Gulf of Mexico about 460 nanotesla per minute.”

“We’ve been in a trend line for many decades, of increasing vulnerability of the US power grid infrastructure to this particular threat.”

Jonathon E. Monken, Director, Illinois Emergency Management Agency (IEMA); Chairman, Central United States Earthquake Consortium (CUSEC)

The final speaker on the panel reviewed work going on now to consider resilience and response planning for another black sky hazard: severe earthquakes. Jonathon Monken spoke of recent planning focused on the risk of a major earthquake in a U.S. Midwest fault zone. “The New Madrid [fault zone], … the most powerful seismic zone in North America, is located between St. Louis and Memphis.” Given the extraordinary projected impact, “This is really a true definition of a complex catastrophe, because it brings together all levels of government.”

Mr. Monken recently participated in the Capstone-14 exercise, which evaluated the impact of such an event. 2.4 million households were projected to be without power due to the direct impact, with a direct economic impact of $296B. By comparison, the estimated impact of Sandy was $64B. Katrina, $106B.

According to utility companies participating in the exercise, primary regional transmission lines would be completely severed and “multiple high-voltage 500 KV transformers [would also fail] due to that combination of both ground shake and the resulting flooding, … and we would see a distribution network that’s ultimately just in shambles.”

Such an event would be extremely stressing for response operations, even relative to other black sky hazards. Recovery from the resulting long duration, large area power outage would be complicated by shattered roads and bridges, broken water and wastewater mains and severe disruption of other interdependent infrastructures. And even without these complications, power restoration would be a massive effort. “We also have the insufficient equipment or trucks nationally to deal with the amount of downed power lines. […] We were forced to fly utility trucks on air force C17s from the west coast to the east coast for Sandy,[…but] this is a much larger magnitude event.”

What were some of the lessons learned from the exercise?

Cross sector coordination will be key. “This is something that really highlights the importance of the synergy and nexus between public and private [sectors],” he said. And with demand outstripping...
resources, prioritization – in the context of cross sector coordination – will be essential. “And … in emergency management priorities, which is my realm of expertise, my tier 1 is transportation and communications.”

Fuel, he explained, will be a critical resource for all priorities. “If you’re going to save as many people as you can. […] what it really translates to is availability of gasoline. That’s going to be our most significant problem.” Ideally, one of the primary tasks of a cross-sector coordination process would be “to try and prioritize that fuel with transportation, communication, life safety, and then number four being utilities. […] So we all share the same Achilles heel, which is fuel.”

And this problem goes beyond fuel availability. “So the biggest problem is the futility of the emergency power system, which is there is no organized regional or national strategy to provide temporary power to an area this large.”

Of course, converting fuel into temporary emergency power requires emergency generators. Along with fuel, backup generators will be crucial in addressing every dimension of a long term outage, and these are also a limited resource. “[Even if available] they have to be supplied by that fuel, and ultimately the existence of a generator does not guarantee operability.”

Thus, coordination of the recovery will be essential. And not just to the communities directly affected. “Six of the top twenty U.S. electricity producing states are actually in the area of impact, so you could imagine taking those offline would have a significant effect.” While the Capstone-14 exercise focused on direct impacts to the New Madridd fault zone states, the impacts on the rest of the country would also be serious – an analysis that has not yet been done. “It will take quite some time before we can even stabilize the national power grid, much less the area of impact.”

For example, “109 million megawatt hours of electricity goes out of the central us grid into the eastern United States.” In addition, “Shipment of coal and oil are heavily dependent on rail line transportation,” and important coal mining regions overlap the New Madrid fault zone.

Perhaps an even greater concern is the earthquake’s impact on fuel pipelines that serve the generating plants of the eastern interconnection. “The main natural gas lines, and the raw crude oil transportation pipelines run through this area of the United States, and supply the bulk of about 75% of the refineries of the north central and northeast United States.” The impact of a shutdown of the bulk of the nation’s natural gas and crude oil pipelines on the rest of the nation’s power grid remains to be evaluated.

“\[There is no organized regional or national strategy to provide temporary power to an area this large.\]”

“\[The main natural gas lines, and the raw crude oil transportation pipelines run through this area of the United States.\]”
Panel 2 | Security Briefings: Manmade Hazards
Part One: Cyber Terrorism: Considering a Sophisticated, Coordinated Threat

The second panel in the session provided security briefings on manmade hazards. In Part One, panelists provided an update on cybersecurity hazards to utility companies. In summary, they said, major utilities in North America are now under continuous and escalating cyber attack – and the attacks include attempts to invade industrial control systems. The most serious attacks come from China and Iran, and it is apparent they are looking at developing and refining their capabilities.

One of the toolsets available for protection is cyber insurance and, in fact, cyber insurance has now expanded into the realm of protection of physical assets of utility companies. These insurance products are designed to respond to major catastrophic events, not just by payment of claims, but also by helping develop incident-response mechanisms to control loss.

Similar insurance products exist for terrorism insurance, and are now under development for EMP events.

How can the insurance aspect of the equation help further? In the panel, it was recommended that an initiative be explored for development of an international body that could help in risk assessment across the cyber world – a process that could help in establishing best practices for protection and response.
Summarizing the current cybersecurity threat in the U.S., Gerry Cauley described an environment that has been changing and evolving rapidly. “Today in North America,” he said, “we are under a continuously escalating threat.” The threat, he said, is a mix of intellectual property threat and denial of service attacks, as well as attempts to get into industrial control systems.

“There has been some limited amount of what I would call experimental activity in the industrial control side, into SCADA systems and RTUs […] of an exploratory nature, trying to figure out if I do this, what will happen, and how would that work. They’re looking at developing capabilities, developing, or experimenting [to see] what they can do.”

“The most serious threats come out of Iran and in China, and if you … study the activity, you see patterns [that indicate] well-coordinated, well-planned, long-term strategies,” Gerry Cauley said. Iran, for example, was behind the attacks on Saudi Aramco and RasGas, and succeeded in launching programs that had serious impacts on cyber assets.

“[This] is a challenge that’s not going to go away, and … continues to grow exponentially.”

What is being done about it? In addition to the GridEx II exercise, described later in this report, “there’s significant amount of mitigation going on. … There’s a growing culture of security within companies. … We have mandatory standards that the Federal Energy Regulatory Commission has approved.” In addition, he said, there is a robust information exchange process taking place, mediated by NERC.

“Today in North America we are under a continuously escalating cybersecurity threat.

“There has been some limited amount of experimental activity in the industrial control side, into SCADA systems and RTUs. They’re looking at developing capabilities, developing, or experimenting to see what they can do.

“The most serious threats come out of Iran and in China, and if you study the activity, you see patterns that indicate well-coordinated, well-planned, long-term strategies.”
David Croom-Johnson, Underwriter, Aegis Insurance Services, Inc.

“I happen to represent a mutual insurer in the gas and electric utility industry. We have 330 members in the US and North America who are mutual members buying from us property casualty … [and] cyber insurance.”

David Croom-Johnson explained that the cyber insurance market is a relatively modern phenomenon, beginning in the late ’90s. And recently, as the threat has evolved, with examples like Stuxnet leading the way, “Cyber [insurance] has moved from what has been network security and data privacy protection … into the protection of the physical assets of utility companies.”

In other words, he explained, this is a new and serious development. Insurance companies like Aegis are being asked to protect the operational assets of utility companies from cyber-attacks. But what roles, he asked, can insurance actually bring to the table?

“Insurance has been pretty good over the years in responding to major catastrophic events, not just by the payment of claims, but also in helping develop incident-response loss control.”

Now that the threat is moving into operational assets, the insurance industry is beginning to take a holistic view of risk assessment. “And if there’s one thing I would call for, with this summit, it is for us to think about an international body that could help in risk assessment across the cyber world.”

There are precedents, Mr. Croom-Johnson pointed out. “If you think: we’ve done it in nuclear. We’ve also done it in marine ….An international body that could set the standards for risk assessment, for incident response, and of course for loss of control [could] help us setting the standards of security in the cyber world.”

Cyber insurance has now moved into the protection of the physical assets of utility companies.

Insurance has been pretty good in responding to major catastrophic events, not just by payment of claims, but also in helping develop incident-response loss control.”

If there’s one thing I would call for, with this summit, it is for us to think about an international body that could help in risk assessment across the cyber world.
This could, itself, be helpful in defining best practices for incident response.

David Croom-Johnson completed his presentation by touching on related hazards. “There is very much a thriving market for terrorism insurance, and that market is looking at and is developing products around EMPs as well,” he said.

He finished with a word of caution. “Risk transfer is what insurance is all about … [However] the insurance industry, even on a global scale, is only going to be a partial solution to any of these issues of cyber terrorism, of EMPs, of cyber-attacks on utility companies. […] The capacity or the limits that we provide in our insurance policies globally will never meet the demands of the social issues that will arise from a major cyber terrorism attack that crosses over a multitude of utility companies.”

What are some next steps? “We want … throughout the insurance industry, to work with partners … [on] the contribution that we hopefully can make to this debate.”

“There is very much a thriving market for terrorism insurance, and that market is looking at and is developing products around EMPs as well.”

“Risk transfer is what insurance is all about. But the insurance industry is only going to be a partial solution, and will never meet the demands of the social issues that will arise from a major cyber terrorism attack that crosses over a multitude of utility companies.”
In the second portion of the “security briefings” panel, Dr. Stockton provided a briefing on the risk of combined arms attacks – with malicious attacks timed to coincide with severe weather events, or with parallel malicious attacks.

The problem? Such attacks could drastically slow power restoration, and given a large-scale event, there are no current plans for providing the scale of security assistance that would be required. Even with such planning there is no capability, today, for situational awareness on the necessary scale, or focused on guiding security personnel.

Finally, addressing both combined arms attacks and other forms of large scale, malicious action against utilities, Dr. Stockton pointed out that, as the Pentagon continues to develop new plans for potential overseas missions, such planning could result in nation-state attacks on infrastructure in the U.S. homeland, to disable overseas capabilities.

Addressing the issue, Dr. Stockton made three recommendations:

• Begin developing plans for large scale security support to power restoration
• Develop enhanced approaches for situational awareness, addressing combined arms missions
• Look at power industry resilience measures addressing serious, nation-state level attacks.

In closing, Dr. Paul Stockton used a quote to help give the answer to concerns that may be summarized, perhaps, as “utility owners should not have to be war-fighters.”

“So let me quote from Leon Trotsky,” Dr. Stockton said. “You may not be interested in war, but war is interested in you.”
Dr. Paul Stockton, Former U.S. Assistant Secretary of Defense

“All the partners in this room face the growing risk of what I’ll call combined arms. That is, in a single event, the adversary will use multiple means to attack the electric power grid, in ways for which we’re poorly prepared.”

While considerable work has been done in the power industry to enhance protection, especially after Sandy, “I believe that we’re not in nearly as good shape in the operational realm.”

We are not well prepared to conduct power restoration efforts during security operations, for example, in response to kinetic attacks combined with serious storms or other disruptive events.

Thanking Gerry Cauley for GridEx II, he highlighted that exercise as an example. “I found it shocking,” he said. “It was a simultaneous cyber and kinetic attack on the electric power grid.”

**Combined arms attacks, in times of severe weather**

Attacks taking place under cover of severe weather events like Sandy, he said, could be a serious problem. “That would greatly increase the duration and geographic scope of power outages, greatly degrade other critical infrastructure in ways for which we’re poorly prepared.”

**Recommendation: Begin developing plans for large-scale security support to power restoration**

What are the gaps? If companies request assistance with security, where would it come from? “Who’s going to provide for the security? When I reached out to the national […] state and local law enforcement associations they told me they’re going to be busy.” In addition, in a black sky-class event, “we can’t count on them providing the kinds of capacity that’s going to be required.”

“Combined arms attacks would greatly increase the duration and geographic scope of power outages, greatly degrade other critical infrastructure in ways for which we’re poorly prepared.

“There are no large-scale plans to provide for this kind of power restoration support.”
And with the limitations imposed by posse comitatus, which forbids the use of federal army forces to enforce the law, these forces would be unavailable to provide the security needed.

Another option would be National Guardsmen on state active duty. “But there are no large-scale plans to provide for this kind of power restoration support. And folks, if you don’t have plans for something, the last thing that you want is to be making those plans up in the midst of an event.”

Recommendation: Enhancements needed for situational awareness

“Secondly, we lack the situational awareness. We lack the kinds of intelligence and information sharing that are going to be required in such an event.”

“Fusion centers or joint terrorism task forces,” he pointed out, “were never created to provide for the operational flow of intelligence that allows humans to know where they need to go.”

“So let’s start getting serious about what it’s going to take to provide for the information analysis and sharing to provide for effective security support to utilities in combined threat.”

Recommendation: Look at power industry resilience measures addressing serious, nation-state level attacks.

“Industry is doing a great job with all of its partners in getting ready for terrorist threats. I don’t believe we’re doing nearly enough against the risk of an attack by a nation state. I know people in industry don’t tend to think that this is their problem. I know governors, states and localities don’t think it’s their problem.”

“It is a problem.”

There are no large-scale plans to provide for this kind of power restoration support. Let’s start getting serious about what it’s going to take to provide the information analysis and sharing for effective security support to utilities in combined threat.

We are not doing nearly enough against the risk of an attack by a nation state. I know people in industry don’t tend to think that this is their problem. ...It is a problem.
Pointing to plans under development to deploy forces “against potentially large Asian powers,” strategists assume there may be attacks on the U.S. homeland to disrupt our ability to operate abroad. “Those attacks could include, very early on, cyber-attacks, or other unconventional attacks on the electric power grid.”

“So let me quote from Leon Trotsky: "You may not be interested in war, but war is interested in you."
In the third portion of the “security briefings” panel, Dr. Ollie Heinonen provided an update on some of the risks associated with nuclear weapon proliferation, as a precursor to the risk of geostrategic EMP threats.

Dr. Heinonen focused his presentation on the status of the nuclear programs in North Korea and Iran. In both cases, he said, there are reasons for continuing concern. Iran, he said, must now be characterized as a nuclear threshold state. And based on what little is known about North Korea, he believes it is now reasonable to assume they have reached the capability for industrial-scale production of enriched uranium, in addition to their developing focus on plutonium production.
Dr. Ollie Heinonen, Former Deputy Director General for Safeguards, IAEA

As the former Deputy Director General for Safeguards at the International Atomic Energy Commission, Dr. Ollie Heinonen remains well informed on the status of nuclear proliferation, worldwide. In his brief presentation, he provided a public domain update on the current trends and concerns.

Beginning with North Korea, he said that Pyongyang is once again producing plutonium. “The reactor there in Yongbyon has been operating for half a year now,” raising new concerns for the rate of production of compact nuclear warheads. In regard to uranium enrichment, “We don’t know very much,” he said. However, their enrichment project began ten years ago, with the help of the Pakistanis. “It normally takes a decade when you reach the ability to produce industrial scale enriched uranium. So we can at this point of time expect that North Korea has that capability.”

It is clear, he said, that “they want to militarize their nuclear devices. There’s a development at the same time, simultaneously for cruise missiles -- ... they want to have a second strike capability in their submarines.”

Iran, he said, “has installed 90,000 fairly simple IR-1 centrifuges which can produce ... high-enriched uranium stocks.” This capability gives them “every two months enough high-enriched uranium for a nuclear weapon.”

In reality, therefore, “Iran has become a nuclear threshold state. On plutonium, he said Tehran has a “heavy water reactor under construction, and work on its components “was not blocked by the ‘Five Plus One’ agreement.”

“There is no assurance for us at this point of time, that those 90,000 centrifuges are the only ones in Iran.”

“Then we know quite a lot of Iran’s missile program. But what is the most puzzling thing is how far they have come with their nuclear weaponization. There has been sporadic information and IAEA has raised the concerns.”
Overall, he said, the real status of their suspected warhead development program is difficult to
determine, due to Tehran’s secrecy. “This is one of the biggest unknowns in my view, in the Iranian
nuclear program.” Beyond that, he expressed concern that
we don’t necessarily know the full scope of their enrichment
capability. “There is no assurance for us at this point of time,
that those 90,000 centrifuges are the only ones in Iran.”

“\[In reality, Iran has become a nuclear threshold state.\]
ONE
GREAT
GEORGE
STREET
Session Two

Status: Where Are We Today?

Status Review:
Planning for a Black Sky Day Power Outage Event
Congressman Trent Franks, an Organizing Cochair of the summit, opened his remarks on a note of optimism. “I think there’s evidence gained on many grounds here that we’re moving forward, and it really encourages me a great deal.”

However, he warned that the United States’ security depends on the civilian electric grid, which remains vulnerable to malicious hazards like EMP. “Such vulnerability is really the kind of thing that invites attack,” he said. And terrorists have learned to target critical infrastructures. “A few weeks ago, we saw attacks on the electrical grid happen in Yemen. Twenty three million people were to find a country without electricity as a result of a suspected tribal attack on vital power lines, … a nationwide power shortage or power outage for that tiny nation.”

Given where we are today, he said he feels this is a soluble problem. “There is still time, still may be time for the free world to address and mitigate the vulnerability that naturally occurring or weaponized EMP represents to the mechanisms of our civilization, without paying an enormous price.”
Panel 1 | Corporate Energy Sector -
Accomplishments and Work
In-Progress

Reviewing today’s status in the corporate energy sector, Dr. Chris Beck, Dr. David Elmakis, Thomas Galloway, Chris Train and Jarmo Elovaara reviewed steps that have been taken, world-wide, to enhance protection against electromagnetic threats and other black sky hazards.

Work on EMP protection began in the 1970’s in Finland, with considerable testing going on today – including laboratory GIC tests of EHV transformers.

In the United Kingdom, the last five years have seen a significant increase in effort to address electromagnetic threats, beginning with a shift to the 1921 “Halloween” storm as the benchmark scenario for the GMD threat. National Grid is also assessing the IEMI threat to their power grid assets.

In the United States, electromagnetic threats are also seeing increasing attention from the energy sector, with workshops focused on GMD and EMP now taking place, helping to formulate a basis for action.
Dr. Chris Beck, Vice President for Policy and Strategic Initiatives, EIS Council

Dr. Chris Beck spoke about EIS Council’s International Electric Grid Protection Report, a recent DOE-sponsored project reviewing international capabilities and best practices addressing electromagnetic threats. These best practices and lessons learned, he said, are directly applicable to the U.S., in spite of the differences in power grid size and complexity. “The physical characteristics of the grid are similar enough that there are lessons we can learn,” he said.

He gave a number of highlights from the Report. The United Kingdom is focusing on GIC withstand, “using a three-limb [EHV transformer] core design where possible. They are monitoring GIC in the system in real time, and they have upgraded their [GIC] design basis threat to the 1921 Railroad Storm versus their initial cut, which was the 1889 Quebec storm.”

“Norway,” he said, “has this regulatory structure which is explicit about protection from GMD and EMP.” And both Sweden and Finland “have implemented an [EHV transformer] GIC-withstand design standard, where the transformer has to be spec’d to be able to withstand 200 amps of DC while fully loaded for ten minutes and not suffer negative thermal impacts.”

He went on to speak of E-threat research that has taken place in Japan and South Korea, GIC measurements now taking place in Australia, and some unique work done in New Zealand. “New Zealand is an interesting case in that they use … grounding resistors … [to limit DC current on] a high-voltage DC link between the north and south islands.” This system also can dampen GIC.

“South Africa has had their problems with the 2003 Halloween storm,” he continued, which made their system an “unfortunate laboratory” that we can learn from. And Israel has done work addressing such hazards on their power grid. Overall, he summarized, there is a surprising amount of information and experience available, worldwide, on practical measures being taken to evaluate and protect against electromagnetic hazards.

“Norway’s regulatory structure is explicit about protection from GMD and EMP.”

“South Africa has had their problems with the 2003 Halloween storm.”

“The United Kingdom has upgraded their GIC design basis threat to the 1921 Railroad Storm.”
Dr. David Elmakis, Senior Vice President, Planning, Development & Technology, Israel Electric Corporation

Dr. David Elmakis provided a detailed update on work done and planned by Israel Electric Corporation, to increase the protection of Israel’s power grid against EMP. His presentation is restricted.
Jarmo Elovaara spoke about GIC policy and experience in Finland. “Fingrid is the national grid operator in Finland,” he said. Fingrid has about 50 400 KV EHV transformers, with their grid interconnected with Sweden and Estonia. The combination of long north-south lines with Finland’s high soil resistivity could lead to serious GIC conditions, particularly given the country’s high northern latitude. However, due to Finland’s concern for earth-fault currents, they have taken design steps that can also address GIC concerns. “If you have an earth-fault in a high-voltage system, you easily create dangerous [voltage levels],” he explained. As a result, he said, from the beginning, Fingrid decided to use exclusively full transformers, rather than autotransformers.

In addition, he said, “We have used in every transformer which is grounded a power-limiting coil. It is not the Petersen coil, so we do not compensate for current. But we limit its magnitude.”

Finland also tests its transformers, with laboratory tests that create “very high leakage flux in the transformer in a way to simulate the path of the DC flux.” In these tests, “we measure the hotspots in the iron core and in the windings, with fiber optics and so on, so we know how our transformer behaves during very strong leakage fluxes or DC fluxes.” As a result, they have demonstrated that their transformers do not develop hotspots exceeding 120 degrees Celsius with a 200-amp DC current in the neutral for ten minutes.

They have measured significant GIC levels due to space weather events. In 1991 “we measured 200 amps in the Rauma transformer neutral point, … but the duration of the spike was very short.” Overall, during the 40 years of measurements, their systems has not experienced a very high, long duration GIC level.

In summary, he said, “We have been studying [and protecting against] GICs since the ’70s, about 40 years now.”
Chris Train, Director, Network Operations; Group Director for Safety, Sustainability, and Resilience at National Grid UK National Grid

Chris Train began by saying the security of the UK national grid is improving, but there is still work to be done. “I think we’re definitely in a better place, but we’re not complacent with the changing nature of the threat.” National Grid continues to evaluate hazard scenarios, and explore both hardening and operational mitigations, with periodic exercises to test their preparedness.

Their increased focus on E-threat protection began fairly recently, he said. “We had a big shift to our approach around this area over the last five years, based on that changing view around the threat assessment.” This involved shifting away from a benchmark space weather event set at the levels of a 1989 storm. “We changed the threat scenario to the 1921 scenario,” he said, a far more severe event. “That kicked off quite a lot of extensive work.” National Grid has reassessed their EHV transformer designs and configurations, based on the new benchmark.

That said, however, “We all recognize there’s still quite a way to go.”

Another step taken is to develop an emergency response coordination body. “One of the things we have done extensively here is worked with something called the Energy Emergency Executive Committee, which is an energy body for the energy industry to look at resilience, from planning for and understanding the threat to continuity of supply, to security of supply.”

Where are we today? “Our operational procedures better reflect the threat than they did previously. We do run exercises every year, so every year every shift team that we have runs through a space weather exercise as a full shift team. We validate our models through having sensors on our substations so that we can improve that validation and calibration. Much more work for us to do in that area.”
National Grid also now addresses the IEMI threat. “We’re looking at the level of IEMI threat that we have against our assets.” And on cyber, he highlighted a substantial change over the last six years. “If I go back probably six years, I think we had two people within the organization responsible for digital risk and security of our important operational systems. Today we have 65,” he said. “Who knows where that is going to end, but I think it is an example of the changing nature of the threat, and the consequence is absolutely enormous.”

Chris Train also referred to the new cooperation between the U.S.’s NOAA and the U.K.’s Met Office. “I was going to say we’re receiving daily reports, but on occasion I’m receiving five or six of them within a day if things are happening.”

In summary, he said, “I think the thing we have to do is beware of creeping risk and the interdependencies, those things you certainly don’t realize occurred.”

““The Energy Emergency Executive Committee addresses resilience, from planning for and understanding the threat to continuity of supply.”

““We’re looking at the level of IEMI threat that we have against our assets.”
Access to effective best practices is essential for expanded resilience to severe hazards. For meaningful progress – especially for the critical, voluntary aspects of such progress, this requires a good, trusted mechanism for sharing such information.

One approach is offered by the North American Transmission Forum. NATF, Tom Galloway explained, provides a number of programs designed to support such sharing. One major area is NATF’s peer-review program, providing expert teams that can help companies review and enhance their performance. “We send teams of about 25 subject-matter experts out to a host member for a week at a time and essentially dissect their performance,” he said. This can be particularly helpful for resiliency and security, where best practices and lessons learned are often particularly relevant, from company to company. For example, “we’ve run a number of security and resiliency related workshops over the last year and half, starting with a severe weather workshop; physical security, GMD 201 and 301 as we called them, and EMP, which was very well attended. I think [the EMP workshop] kind of helped a lot of our members turn the corner in terms of the recognition of that as a real threat and something that we need to act on.”

NATF also hosted a cyber-security workshop, “and we’re building towards a capstone resiliency summit this October,” giving them a key role in hosting information sharing addressing all of the black sky hazards.

“We’re focused on a bias for action,” he said. “We’re not going to admire the problem anymore. We’re going to move forward. And we’re going to look at this from an all-hazards perspective, across four different modes as we’ve defined them: assess, prevent, detect, and recover.”

“[The EMP workshop] helped our members turn the corner in recognition of that as a real threat and something that we need to act on.

“We’ve run a number of security and resiliency related workshops over the last year and half: severe weather, physical security, GMD and EMP, which was very well attended.

“We’re focused on a bias for action. We’re not going to admire the problem anymore.
Bill Bryan, Joe McClelland, Roger Steen and Dr. Shlomo Wald continued the review of “Where we are today,” addressing the government sector. Governments typically collect and analyze information defining the changing threat environment, while also providing leadership and coordination in protecting against such hazards. Panelists discussed the challenges of addressing black sky hazards from both of these perspectives.

Reviewing the threat environment, panelists warned that, according to news reports, cyber threats designed to invade infrastructure control systems have been rapidly increasing. At the same time, continued improvements in infrastructure connectivity and efficiency have tended to make these infrastructure systems more vulnerable to such threats.

Electromagnetic threats were also discussed. Severe solar weather represents a serious concern for the U.S. high voltage transmission systems. And in regard to EMP and IEMI, access to electromagnetic threats has increased.

In this environment, information sharing and coordination is particularly important, and panelists from Norway and Israel offered examples, based on the work going on in their countries. Israel uses a non-probabilistic approach to assess likelihood of severe threats. Norway has had EMP regulatory rules in place since 1970, mandating protection for SCADA systems, and requiring companies to model their vulnerability to GIC. Norway also has a nation-wide, EMP-protected communication system, independent of public carriers, resident in energy company facilities.
Joe McClelland began by pointing out FERC’s unique role in addressing resilience and security issues broadly across the U.S. energy domain. “FERC … issues license and certificates for oil and natural gas pipelines, liquefied natural-gas terminals, and dams. In addition, it has specific oversight authority for the reliability and security of the bulk power system.”

Given this broad perspective, the FERC Office of Energy Infrastructure Security addresses concerns and best practices associated with a broad set of black sky hazards.

For some, he explained, “the Commission decided that these threats require special treatment.” One example is cyber. “As far back as 2007, the Department of Homeland Security and Idaho National Lab demonstrated that a cyber-attack could damage or destroy generators. From that time, there have been sophisticated and effective real-world attacks on industrial control systems.”

He referred to ongoing news reports on cyber-attacks designed to manipulate industrial control systems. According to such news reports, he said, many such programs “have been specifically directed at industrial control systems and energy infrastructure. Programs like these can enable an adversary to shut down energy infrastructure to sites that ensure our nation’s public safety, economy, and defense.”

Intentional Electromagnetic Interference (IEMI) weapons have also been in the news, he said. “There were news articles in late 2012 reporting the very successful testing of CHAMP … a missile that uses microwaves to target electronics and control systems. In fact, there are reports that nearly two-dozen countries are developing e-bombs, capable of wiping out computers and electronics, including those that control a nation’s vital services, such as finance, telecommunications, water, sewage, and energy infrastructure.”

According to news reports, programs “have been directed at industrial control systems and energy infrastructure to enable an adversary to shut down energy infrastructure to sites that ensure our nation’s public safety, economy, and defense.”

Our vital infrastructure today “has increased in both efficiency and automation. With these changes comes increased risk.”
On kinetic attack, “recent news reports have detailed a more traditional kinetic attack on transmission facilities in Yemen that plunged the entire country into a blackout.”

And there are natural hazards that can directly and preferentially affect the power industry. “Coronal-mass ejections can play havoc with the earth’s magnetic field, thereby generating ground currents that can damage and destroy vital power-grid equipment, causing wide-area power interruptions.”

There are two sides, of course to infrastructure resilience. While severe hazards have been expanding, improvements in the efficiency and productivity of lifeline infrastructures have often come at the expense of greater vulnerability to such hazards. Our vital infrastructure today “has increased [in] both efficiency and automation,” McClelland said.

“Natural-gas power generation has almost doubled, from 16% in 2000 to 31% in 2012. [The] 35 million smart meters in service today in the United States [are] expected to double to 67 million smart meters by 2015. Now, with these changes comes increased risk.”

He then went on to give examples. “Increased gas usage without redundancy, storage, or fuel diversity can mean new and larger single points of failure. Increased automation means increased cybersecurity [concerns] and millions of new onramps to critical infrastructure, and new susceptibilities to electromagnetic pulse events. Greater transformer efficiencies can mean less spares because of interchangeability, or even increased geomagnetic disturbance susceptibility.”

“Largely due to Chairman LaFleur’s dedication, FERC has passed regulations to increase the resiliency of the energy infrastructure through new standards developed by NERC, with Gerry Cauley and his help. The standards are aimed at strengthening the foundational practices for the users, owners, and operators at the power grid for cyber and non-cyber threats and kinetic attack or natural geomagnetic events.”

And of course, he went on, the Office of Energy Infrastructure Security was established, “and has been working with other agencies such as DOE, DHS, and others, and the states, the regulatory community, and other stakeholders to help develop best practices for applications at the most critical facilities.”

In conclusion, he said, “Considering the broad base and sophistication by which a cyber, physical, or electromagnetic threat can occur on the energy infrastructure, it’s important for all affected to share information and coordinate actions.”

“Nearly two-dozen countries are developing e-bombs, capable of wiping out computers that control a nation’s vital services.”

“Coronal-mass ejections can generate ground currents that can damage and destroy vital power-grid equipment, causing wide-area power interruptions.”

“Considering the broad base and sophistication by which a cyber, physical, or electromagnetic threat can occur on the energy infrastructure, it’s important for all affected to share information and coordinate actions.”
Bill Bryan spoke about resilience, and the impact of lessons learned from serious events like Rita, and Katrina, and Superstorm Sandy. “It’s estimated that 18% of the US population lost power during Sandy,” he said. “And I can assure you that with all that’s gone on since Sandy, if New York and New Jersey were to experience another storm similar to that, they will be better prepared.”

These experiences have created a new focus on resilience. And a key element is preparedness. “There needs to be better preparedness at all levels,” he said, in both the government and private sectors. Another key lesson learned was the need for improved resources to enable response operations. In particular, “better situational awareness and information sharing. It just wasn’t there.” And one of the key problems was that, with all the people involved, many stakeholders were simply unaware of the existing mechanisms to support that process, “not really recognizing the national response mechanisms that are already in place to share information.

And, closely related to this, the importance of training and exercises. “If you’re going to have a plan, you’ve got to exercise the plan.”

In summary, he pointed out, from preparedness before an event, to comprehensive, well-communicated plans to enable situational awareness and information sharing during an event, “it is about managing risk.” To manage risk, preparedness and planning all has to take place, and be well-exercised, before an event.

“When firemen go out to put out forest fires, they rarely put out the fire, but they shape the forest, and the fire ultimately dies out.”

“We have to look at each one of these things that threaten our grid, whether it’s EMP, whether it’s cyber, whether it’s physical attack, whether it’s a severe weather event, and we have to shape that forest for that event.”

“It’s going to come.”
Dr. Wald used EMP as an example, representing the full set of black sky hazards that can affect many infrastructures over a large area.

“The broad mission of his ministry is to supply sustainably the energy, water, natural resource needs … regularly and in case of emergency, … and in compliance with environmental standards, and in a way that it is economically viable.”

A key element of this is to plan appropriately for emergencies that can result from major threats or hazards. In Israel, such threats are identified through a formal process. “The government defines what are called reference threats.” And while work has already taken place, “[EMP], for example, is not yet defined as a reference threat.”

Dr. Wald pointed out that the normal, probabilistic prioritization process for typical threats is inappropriate when dealing with uniquely serious, deterministic threats. A “deterministic threat,” he explained, is “something that … if it happens, it’s something that we can’t afford.”

EMP is a good example of such a threat, mandating development of a mitigation program. In fact, he pointed out, since EMP mitigation efforts would be designed for recovery, and would not require continuous continuity of operations, the investments required would be economically viable.

In Israel, the process was kicked off two years previously, he said, with efforts from both EIS Council and the Israel Electric Company, leading to historic and projected mitigation efforts. This is now a subject of broad corporate and government interest. “A joint EMP forum [of] about ten governmental bodies [is now discussing and promoting] the capabilities of Israel to mitigate EMP.”

And EMP, he reiterated, simply represents the full class of severe infrastructure hazards. “If we should be prepared for the malicious EMP attack, then we shall eventually be able to mitigate also the other [severe hazards] that can happen and affect the grid.”

“A deterministic threat like EMP is something that, if it happens, it’s something that we can’t afford.”

“A joint EMP forum of about ten governmental bodies is now discussing and promoting the capabilities of Israel to mitigate EMP.”
Norway has had a particular focus on power grid security for many years, Mr. Steen pointed out. In large part because of the high dependency on electricity for essential heating. “Norway can be a little bit chilly, cold during the wintertime, and … a quarter of the nation [for heating, is] 100% dependent on stable electricity.” As a result, he said, Norway’s power grid regulations include “specifically protection … against natural disaster, technical failure, and manmade threats.” Manmade threats can be [malicious threats] but also from foolishness or malfunctioning.”

EMP [including IEMI] is one of the malicious threats included in Norway’s power grid regulatory requirements. “EMP … regulation in Norway [began in the] 1960s. It started as [a] military threat when they start to [test] nuclear bombs up in the atmosphere. […] So we started the regulations I think it was in 1970 up to today.” For example, “all SCADA systems should be protected against EMP and EMI. So every SCADA system is built in secure facilities.”

Similarly, he said, “[In regard to] GIC in the transformer and grid system, all companies need to evaluate the consequences of GIC. They have to carry out risk analysis to see if there’s any problem. And if the conclusion is yes, we have a problem, they have to do something to lower the probability or lower the consequences.”

For any severe hazard, communication will be key. “We also have our own communication system within the energy companies in Norway, and they call it the most important system, both for the users and the biggest grid companies. So we manage to communicate nationally on a secure telephone system that is independent of public providers […] that gives us the opportunity to start up from a total blackout situation if it should happen.” And this communication system is also EMP protected. “Most of this

“EMP regulation in Norway started in 1970 [and continues] to today.

“All SCADA systems should be protected against EMP and EMI. Every SCADA system is built in secure facilities.

“All companies need to evaluate the consequences of GIC. And if the conclusion is yes, we have a problem, they have to do something to lower the probability or lower the consequences.
communication system is protected like the SCADA system, in secure facilities, [giving us] end-to-end protection."

Other regulations relevant to severe hazards address a variety of concerns. For example, “We added a new requirement in the regulation that we need two independent sources of timing if you are dependent on GPS timing. We have two different reasons. One is space weather, but you also have this possibility for what you call GPS spoofing or trying to manipulate time.”

Following Mr. Steen’s presentation, Congressman Franks asked if he could go into more detail on the standard Norway uses for hardening their SCADA systems against EMP and IEMI. “The standards [include putting] them in rooms that are totally shielded from exposure from EMP. And the standards we’ve used in the energy sector are very close to the standards military use for protecting their systems.”

“…We also have our own secure, EMP protected, national communication system within the energy companies in Norway … that is independent of public providers so we can start up from a total blackout. They call it the most important system.”
Miles Keogh and Commissioner Kelly Speakes-Backman discussed State utility regulatory approaches, and how they relate to resilience investment for black sky hazards. Moving this process forward with regulators, they pointed out, will require finding ways to adapt today’s paradigm to the evolving reality of growing, severe hazards.

The current regulatory environment focuses on delivering electricity, water and other essential services to consumers a cost that is optimized for “conventional” threats. For black sky hazards, this historic approach tends to break down. In fact, regulatory commissions today depend on a normative set of metrics that do not account for very severe hazards.

Addressing these challenges will require developing innovative approaches to better inform utility commissions about these severe hazards, and options for incremental improvements in resilience to these hazards.
Miles Keogh, Director of Grants and Research, National Regulatory Commissioners Association (NARUC)

Miles Keogh spoke to structural realities in the way U.S. regulatory commissions generally operate, that have never been optimized to address resilience needs for severe black sky hazards.

“So why are we dealing with these resilience questions? … One of the problems is that we are talking about … a series of risks that are different than what we’ve been talking about in the past. They are larger in scale. They are unconventional in their origin. And the kinds of ways that we’ve evaluated reliable service begin to break down.”

For this reason, he said, for large scale risks like cybersecurity, EMP, increasing hurricanes and large scale storms, “the resilience strategies that best protect [against] those nontraditional and large-scale risks are particularly vulnerable to being underpriced, using the reliability stuff that we use right now. We tend to underprice those investments.”

For this to change, he suggested, stakeholders need to find ways to communicate this changing reality to decision makers. “Because if you want to make the investment, you have to persuade the regulator that it’s worth it.” And such communication needs to be couched in a format that is meaningful to regulators, he explained. “Is it a problem? Is it one we can fix? What’s the right fix? You need to be able to propose … the right fix at the least cost because we can’t fix everything.”

“… We are talking about a series of risks that are different than what we’ve been talking about in the past. They are larger in scale. They are unconventional in their origin. The ways that we’ve evaluated reliable service begin to break down.

“If you want to make the investment, you have to persuade the regulator that it’s worth it.”
State regulatory commissions, Commissioner Speakes-Backman explained, have a unique perspective, different from their federal colleagues. “We are very close to load, and we are close to demand.”

“In Maryland, … We’re at a nexus of change with respect to the economy, the environment, and the reliability risks. [And] as a result of expiration of certain rate caps, [we are] seeing a 75% increase in rates for consumers for half of our state.” In this environment, regulators are faced with the “competing interests of resilience and reliability and environment and resource adequacy, balanced against the immediate impacts of rate increases. [These] are all topics that have kept me up at night.”

How do they approach this? “We’ve shifted to try to address this to hold our utilities accountable for performance as well as spending… we’re starting to rethink the process of cost recovery. […] We want to know that that spending has been effective, not just spent according to budget.”

In Maryland, the need to develop new, effective approaches to making such complex decisions has been driven by a series of major events. “In the span of only a few years we experienced Hurricane Irene, Snowmageddon, Derecho, Hurricane Sandy, and the Polar Vortex, and those were just the big ones that we gave names to. … It just became really obvious,” she said, that there was a significant and an unsatisfactory disconnect between the public’s expectations of reliability and resilience, and … what our utilities were giving us.”

What does this mean? “So to fix this requires investment, and here’s where I think we’re connecting.” The Commissioner went on to explain that, under the current structure, there is direct competition between resilience investment and optimizing day-to-day rates. “To help us to analyze this, we started with a very rudimentary risk analysis. … We ordered our utilities to make a number of staffing and shorter-
term improvements over … five years. And we allowed them concurrent recovery to help us to minimize the cost of financing this work.”

For long term resilience, “We’ll be holding hearings on the long-term plans that our investor-owned utilities and large co-ops will have to undergo.” However, she warned, “It’s not a black-sky occurrence that we’re measuring for. We’re only measuring for up to 40% [outages].”

To go further, she said, “We’ve got to find out how do we spend money on prevention and recovery when we plan for low frequency, [severe events]. … I realize and recognize that we have to spend money on [high impact scenarios]. But we’re trying to keep the wheels on the bus and the lug nuts are rusting at times. And we’ve got to take care of that too.”

Commissioner Speakes-Backman also echoed Miles Keogh’s comments about the inadequacy of typical value-assessment metrics to address resilience investments for black sky hazards. “In trying to work through the efficiency of spending, we’re looking at the normal measurements … that don’t necessarily apply correctly to catastrophic events. So we’re trying to look at what sort of measurements can we use to employ the methodology that Dr. Wald mentioned. … We don’t yet have them for the objective and real requirements of our utilities in black-sky days.”

“But we’re working through that,” she said, “and I expect we should get through that in the summer.”
Session Three

Policy Implications

The Elements of Good Public Policy for National Grid Security
Keynote Speakers

Summit keynote speakers Assistant Secretary Caitlin Durkovich and Chairman Cheryl LaFleur discussed key government roles in the complex public – private partnerships that mediate critical national infrastructures.

While the power grid and fuel resources in the U.S. are largely privately owned, the security of these infrastructures is supported by voluntary coordination with government agencies and also, to varying degrees by State and Federal regulatory structures. This tension between private ownership and government regulation underlies most aspects of energy security in the United States.

FERC’s ongoing work to develop GMD requirements provides an example of this tension, with regulatory requirements being developed that prioritize critical facilities, and include inherent flexibility, with asset owners responsible to conduct their own vulnerability assessments and develop protection plans relevant to their unique circumstances. The situation is similar for cyber and for physical security.

The overarching reality driving this approach: The recognition that regulation only plays a partial role in infrastructure security.

Thus, voluntary partnerships are key to infrastructure resilience and security. To a large extent, non-regulatory government agencies see their roles as supporting owners and operators, providing tools and training to help mitigate hazards to their systems. And to be effective, experience has shown this voluntary coordination process must include the highest levels of government and corporate management.

Ultimately, regulatory limits provide a foundation, not a comprehensive solution for infrastructure security. As a result, structures that help tie together corporations, government agencies and NGOs are essential to the protection and recovery planning for critical utilities. This “whole-of-community” approach has become a shared vision that underlies the National Infrastructure Protection Plan.
Assistant Secretary Caitlin Durkovich opened her remarks by highlighting the important role of public-private partnerships for emergency response. “My office is primarily responsible for sustaining those voluntary partnerships with owners and operators of critical infrastructure. And so I think public policy is very much a public-private issue, a public-private partnership.”

Much of government’s role in infrastructure resilience emerges from this duality, addressing infrastructure that, while generally privately owned, is critical to the security and continuity of the nation. “The majority of the nation’s critical infrastructure is owned and operated by the private sector, … but at the end of the day, it is essential to national security. It is essential to economic prosperity. It is essential to the resilience of our communities.”

This duality must be a key driver in the way the government engages with industry. “Therefore,” she said, “it is incumbent on the federal government to work in support of owners and operators, to help them understand the strategic risk environment, to share information, and to provide tools, training, and exercises to help mitigate that risk.”

There has been considerable attention given to addressing that relationship. “The National Infrastructure Protection Plan is really the framework that governs how we think about our relationship with the private sector,” she said. And given the importance of this public-private dynamic, this plan was developed as a coordinated process. “[for] Presidential Policy Directive (PDD) 21 -- Critical Infrastructure, Security, and Resilience[…] one of the actions that came out of PPD-21 was a call to update the National Infrastructure Protection Plan[…]. We drafted this new version with owners and operators in the room. … We tried to do it with them as our partners, and with this notion again that we are
managing risk, that there are a number of threats and hazards that can impact the functioning of critical infrastructure.”

However, the public – private axis is only one dimension among many that must be taken into account in developing approaches for infrastructure resilience. Government resources and responsibilities in the U.S. run from federal to state to local levels. “We have to think about it both from a national level but also recognize that risk management happens at a regional level, at a state level, a local level, and certainly within enterprises.”

After framing the planning process, Assistant Secretary Durkovich summarized highlights of the infrastructure protection plan. “The updated National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience … reinforces this whole-of-community approach, and a shared or a joint vision for how you manage risk, with three main pillars.”

The first pillar addresses core needs of the public-private axis. “The first pillar is really information sharing. … We’ve recognized that that has to be a bidirectional flow, that we as government can’t just ask industry for what they’re seeing, the attacks they’re experiencing, and not give something back. … we are providing real-time or near-real-time information, situational awareness to owners and operators of critical infrastructure.” This can be important, she explained, not just to help in assessing a particular incident, but in projecting “the cascading impacts of that incident, and the … measures that they can put in place to mitigate the potential impacts.”

The second pillar, she continued, is interdependencies. “In particular, interdependencies between lifeline functions. … There is a recognition that there are certain sectors that in some ways are first among equal, that really without them, if you pulled one of them out it would be difficult to go about our daily lives.” What are these systems? “Energy, telecommunications, water and transportation.”
Understanding these interdependencies is a prerequisite to preparing for government support to the resilience of critical infrastructures. How is this done? “Within the Office of Infrastructure Protection,” she said, “we are able to do vulnerability assessments on owners and operators of critical infrastructure.” And not only on security policy, but on their interdependencies with other infrastructures. “So if we’re faced with whether it’s a natural disaster or another significant event, we can better understand … the cascading effects of a disruption. … It provides a decision support tool,” she explained.

The third pillar addresses the internal government dimension in supporting critical infrastructure, “this notion again of regional and local. While we spend a lot of time working together in the inner agency in Washington to solve some of these problems, at the end of the day, all of these incidents are local. The dynamics, the particular environment of the owners and operators that we work with are dependent on where they are.”

Regional variations can run from differences in the heuristics of extreme weather or other severe hazards to differences in population, or age and resilience investment in critical infrastructure. “And while we’re working at the national level, there are a lot of regional and local public-private partnerships that can be brought to bear.”

These three pillars define the basic structure of the NIPP. It is essential to keep in mind, however, that the NIPP is not imposed on owners and operators. “The NIPP is … based on voluntary partnerships. And we are working closely through the NIPP now to work with our owners and operators, to set some joint priorities, which really frame our work plan for the next 12-18 months.”

At the end of her remarks, Assistant Secretary Caitlin Durkovich reviewed the value-added of the government support to industry mediated by the NIPP. “We have redefined really how we are engaging our partners … over the course of the last several years.”

The engagement is based on a few simple tenets. Trust, simple processes, and direct engagements with CEOs and chief risk officers. “What we’re learning is that you need the people in that corporate suite who are looking at enterprise risk, who are dealing with brand risk, regulatory risk, operational risk, and who at the end of the day control the purse strings. When you bring them into the conversation … It makes it easier for the chief information security officers to advance their agenda.”

And classified information sharing with senior corporate officials is not the only priority. “We have to learn how to share information at the unclassified level. I guarantee you, you are not missing anything if you do not have a security clearance.”

Finally, the Assistant Secretary focused on the Electricity Sub-Sector Coordinating Counsel under the leadership of DOE, which includes government executives and 40 CEOs from utilities of all sizes. “We give them an update on the evolving threat picture. And I think what has made this group so successful is two things.” The two key factors, she went on to explain, include trust, based on the joint participation of senior officials from both government and industry. “Dan Poneman is always there. I’m always there. My boss is always there. The White House is always there, and our colleagues from NERC and FERC and the FBI.”

Assistant Secretary Durkovich, concluding her remarks, returned to the theme she began with. “I think the best piece, frankly, of public policy, is government and industry working together in tandem.”
Cheryl Lafleur, Acting Chairman, Federal Energy Regulatory Commission, U.S.

FERC Chairman LaFleur focused her keynote address on FERC’s recent activity addressing several severe hazards to the bulk transmission system.

“At the Federal Energy Regulatory Commission,” she said, “we regulate the wholesale, bulk, and high-voltage transmission system, as well as gas and oil and some other areas.” This gives FERC a unique capability to address a wide set of energy assets, including fuel resources and electricity generation and distribution. “The bulk electric system, high-voltage transmission and nuclear units are the only two elements of our critical infrastructure that are subject to mandatory standards at this time.”

Within this broad framework, over the last year FERC approved a set of standards addressing geomagnetic disturbances on the bulk electric system. Over the last year, “the first set of standards was submitted,” she said. “[It] was approved by the Commission last week ... with respect to operating procedures that asset owners and operators in the United States have to have in effect in case there’s a solar storm.” The next phase will go further. “The second part of our requirement of mandatory standards is the hard one. ... Requiring a standard that would require each asset owner to conduct system vulnerability assessments, and come up with a plan to help protect against instability and cascading outages on the bulk electric system as a result of solar storms and geomagnetic disturbances.” That second phase will go beyond training or operating procedures, requiring embedded hardware measures.

For FERC, this is very recent example of a process that has been used for a wide variety of other parameters. “In the cybersecurity

“... The second part of our GMD requirement would require each asset owner to conduct system vulnerability assessments, and come up with a plan to help protect against instability and cascading outages on the bulk electric system as a result of solar storms and geomagnetic disturbances.

“... We regulate the wholesale, bulk, and high-voltage transmission system, as well as gas and oil and some other areas. The bulk electric system and nuclear units are the only two elements of our critical infrastructure that are subject to mandatory standards at this time.
Chairman LaFleur explained that the current cyber standard is CIPP5. “It’s the first Critical Infrastructure Standard that … protects all the assets of the bulk electric system to some extent, but tiers them into high impact, medium impact, and low impact assets, with different levels of protection.”

Beyond space weather and cyber threats, FERC has also been active in addressing physical security. “In March FERC voted out an order requiring NERC and the industry to file mandatory standards for physical security within 90 days, …They did file early on May 23rd, and we look forward to taking that up,” she said.

In all of these, FERC’s objective – and the basis for prioritization of protection efforts – is “criticality to the bulk electric system. Our mandate is for the stability of the grid, and that’s how we judge criticality for our standards.” The Chairman spoke of a tiered process. Rather than requiring universal requirements affecting all comparable components, FERC has been working to ensure protective measures are focused, first, on critical hardware. “So what we’re seeing in the United States across cybersecurity, physical security, and now with the forthcoming rules on geomagnetic disturbances, a focus on what are the most critical facilities, and we’ll protect those first.”

But criticality, she said, is judged in terms of resilience. Rather than considering individual pieces of the system separately, FERC’s priority is to ensure steps taken enhance the resilience of the overall bulk electricity system. “Resilience, the ability to bounce back after something bad happened. … We’re increasingly recognizing it’s not a matter of scatter-shot standards -- … do this on cyber, do this on GMD, we’re going to do something on EMP. But looking across the different risks and seeing what are the things that go into resilience.”

Making “resilience” the key prioritization metric only makes sense of all the elements needed are addressed. Thus, she said, FERC’s perspective spans many aspects of the system. “It’s how you plan

“In March FERC voted out an order requiring NERC and the industry to file mandatory standards for physical security.

“Across cybersecurity, physical security, and now with the forthcoming rules on geomagnetic disturbances, we’re seeing a focus on what are the most critical facilities, and we’ll protect those first.
and design the system in the first place,” building security and restoration planning into the basic system configuration. And, she continued, “Maintenance … [including] training and preparation. “Real-time operation, the folks in the control room…. Response and recovery. It’s also inventory management.” In sum, she explained, “we’re thinking more broadly across the risks, and I think Avi’s right on trend. He’s right on trend in increasing the scope of this conference to the broader topic of resilience. That is where I see more and more the discussion is going.”

And if the objective is resilience of the entire system, far more will need to be brought to the table than FERC regulation. “I think I will echo what everyone has said,” she concluded. “That all of these issues cannot be addressed in isolation by the Federal Energy Regulatory Commission, cannot be addressed in isolation by the United States.”

“It requires a broad response across nations and across the government, state, and federal, and local, the asset owners, the regional transmission operators, first responders, non-governmental responders like Red Cross who were very, very involved in every major emergency, really around the world, and many others. And really getting them all involved in the plan if something bad happens, which is a part of what we have to do.”
Panel 1 | Government Perspectives

Dr. Peter Pry, the Rt. Hon. Andrew Miller MP, Assistant Secretary Todd Rosenblum and Dr. Dan Weinstock explored policy implications of black sky hazards, associated with infrastructure security, from a government perspective. One of the primary messages was the reality that, in the modern world, malicious threats to our critical infrastructures are real.

Another theme, paralleling this concern, was more positive. Approaches for resilience are available and could be implemented. And since, as always, prioritization will be important, government agencies can play an important role in helping with this tiering process.
Mr. Miller had praise for the improving public–private partnerships in the U.S. on infrastructure protection. Nevertheless, he pointed out, “There are pockets of fantastic activity going on, but we need to reinforce this, and get this message beyond the handful of countries that are represented in this room.”

Focusing on severe space weather, Mr. Miller displayed NASA photos of recent coronal mass ejections that had the potential to cause very serious consequences, had they been directed toward earth. He gave a very recent example, from the 13th of June 2013. This, he pointed out, “was a major, major event that was well recorded. The good news is that by an element of chance that Friday the 13th didn’t turn out to be the disaster that it could have done.”

“We really do need to look at a strategy that brings together the best scientific brains from both the public and the private sector and help understand the risks of hazards like severe-space weather, but also military-associated issues such as EMP.”

“We need to bring together the best scientific brains from both the public and the private sector and help understand the risks of hazards like severe-space weather, but also military-associated issues such as EMP.”
“In March of 2013, in the aftermath of North Korea’s 30 illegal nuclear tests. North Korea threatened to make nuclear strikes on the United States,” Dr. Pry began. He also referred to reported conclusions of the defense intelligence agency and CIA that North Korea had warheads and delivery systems that could be used in an attack, and to an assessment by the Congressional EMP Commission that North Korea may already have developed ‘super EMP’ warheads.

Dr. Pry referred to several potential indications, beyond the direct threats of March 2013, that North Korea may be developing logistics capabilities to launch EMP attacks on the U.S., using a variety of delivery approaches.

He also suggested that the idea of inducing large regional power outages as an effective weapon is growing in currency. “A few days before Halloween, October 27th, 2013. A terrorist drug cartel … in Mexico blacked out a whole province. And at the same time,” he continued, terrorists “blacked out the whole country of Yemen … the first time in history that a terrorist attack on the grid has actually blacked out an entire nation.”

Referring to a list of similar indicators, “The pieces are all coming together,” he said. “[However] I think we, as a civilization, are suffering from a failure of strategic imagination.”


“I think we, as a civilization, are suffering from a failure of strategic imagination.”
Assistant Secretary Rosenblum focused his remarks on two areas – a new aspect of the threat of coordinated physical attack on critical infrastructure and, DoD’s approach to risk management.

He referred to growing concerns that Americans and citizens of allied states may become involved in terrorist and rogue state activities abroad, and represent a serious risk to critical assets after they legally enter the U.S.

“I want to underscore it because it relates to resiliency issues, threat issues, vulnerability issues. … And that’s the bleed out of Europeans and North Americans … going to the fight in Syria, making all sorts of associations and connections, and then coming back home.”

The primary concern is not what he called “a classic sort of terrorism threat … “The real concern is for legally resident terrorists “[with] honed skill sets such as the ability to take down … communications towers. To blow up pipelines, launch improvised explosive devices and vehicle-borne explosive devices.”

On risk management he explained that risk management is focused on mission assurance. “The first DOD strategy ever on Mission Assurance was published by Dr. Stockton in 2012.”

DOD prioritizes mission assurance by considering requirements sector by sector. “The first sector of concern for us, obviously, is force protection. [Other sectors include] protecting the people, physical safety, energy, communications, transportation, cyber, insider threats … a whole series of sectors that we look at.” For each of these sectors, he explained, DOD looks at their importance in accomplishing high priority war plans. “What are the assets that undergird our ability to achieve success in those missions?”

And while “in many cases, we will build our own redundancies – microgrids, or transportation -- … the hard truth is we cannot mitigate against all threats.”

As a result, the Department of Defense is increasingly looking at forming partnerships to address those risks they do not directly address. “But ultimately what we need is resiliency and surety of the capabilities that we need to wage war and win war.”
Dr. Dan Weinstock, Former Director, Electricity Authority, Minister of National Infrastructures, Israel

Dr. Weinstock discussed administrative aspects of protection against severe, emerging hazards like EMP. One consideration, he said, is that – regardless of which agencies or ministries should be involved – typically such engagement will only occur if there is adequate domain knowledge to address the hazard. “So the knowledge, lack of knowledge is the first problem.”

The second problem? For an emerging threat, understanding the strategic risk is typically essential. “The Ministry of Defense in Israel of course knows a lot about threats to Israel, but … almost nothing about the electricity system.”

These, he said in summary, are classic issues in addressing any emerging hazard. In Israel, these concerns are addressed, in part, by development of a formal “National Threat Reference Scenario.” This process can improve the understanding of the strategic risk. “Once the [EMP] threat to the electricity system will be part of this document, this is the beginning of the solution. Because this is the document that the decision makers, including the Prime Minister, know, read, and care about.”

Dr. Weinstock also pointed out that it can be helpful to combine resilience strategies for emerging threats with other accepted, better-known or more mature systems. “For example, renewable energy. No one can stop the sun from rising or the wind from blowing, so we can explain that renewable is somehow connected to the security [against the emerging threat].”

Smart grid architectures are also relevant here. While such architectures could be a liability for threats such as cyber, if properly implemented, it could become a synergistic asset with other measures. “Some smart measures can contribute to faster healing of the electricity system after a disruption. I was part of a team that wrote the smart grid roadmap for Israel, and I was amazed at how many technologies can contribute to the security of the electricity system.”

Once the EMP threat is part of this [reference threat] document, this is the beginning of the solution. This is the document that the decision makers, including the Prime Minister, know, read, and care about.

Some smart measures can contribute to faster healing of the electricity system after a disruption.
Sanjay Bose, Terry Boston, Gerry Cauley, John Houston and David Owens came together as a panel to discuss corporate perspectives on policy, in regard to preparing for black sky hazards.

Given the extraordinary experience base represented by the panel, there were many examples of severe hazards, and lessons learned in the recovery process. And while this has provided a foundation for what will be needed to address far more severe, long duration outages, it was broadly recognized that the challenges of black sky hazards mandate new policies and approaches. Above all, the panelists articulated a “call to action,” to move beyond generalities, and begin putting in place the resilience measures and whole community planning that will be essential for these hazards.

What does that mean? One lesson learned has been that people typically cannot tolerate power outages beyond a few days. Regardless of restoration planning, there is work to do in educating the public, and preparing a public communication plan for use during the recovery.

Many panelists spoke the importance of addressing EMP/IEMI and Severe Space Weather, as emerging threats that need to be “taken off the table.” As part of this, there is a need for more information on unique technical and protective approaches for these hazards as well as for advanced cybersecurity and physical hazards, with speakers pointing to a historic lack of information sharing on both protective strategies and specific measures. Making progress will require multiple dimensions of action, and where regulatory measures play a role, panelists suggested, a flexible approach will be important. Overall, between any regulatory benchmarks and corporate initiative, the protection levels implemented must, panelists suggested, be sufficient to properly address such emerging hazards.
Superstorm Sandy was discussed as a watershed event when, for the first time, the power industry was invited to participate directly in the FEMA process. The reality of that process, given the impact of Sandy, made it clear that well-defined leadership will be essential for future severe power outage events.

Many specific lessons learned came from the Sandy experience.

Advance planning is needed to support and expedite utility crews, including the use of DOD facilities. The Stafford Act, which mediates FEMA’s ability to provide federal aid in disasters, deserves review to consider constraints on assisting utilities. And since much of the restoration process in any recovery will include the need to replace equipment, new policies and approaches are needed to define requirements for critical spares for different hazards. This includes providing for cross-corporate and cross-jurisdictional inventories, access and transportation of these spares. New sparing policies were highlighted as a particularly important consideration for an EMP event.

Emergency communication was also identified as a serious gap.

Given that the policies and resilience measures needed for black sky hazards are implemented, training will then be critical. And finally, for any of this to take place, ways must be found to allow for associated cost recovery.
“Forty years ago today I moved into an underground bunker that was designed for a direct nuclear attack from the Soviets, following the missiles of October 1962. We were more prepared then, perhaps, than we are today, even though I do still have two underground bunkers.”

Terry Boston reviewed several black sky hazards, referring to his personal experiences dealing with many threats. “I was pretty sure I had seen everything, from Hurricane Andrew to Hurricane Katrina with 150 mile-an-hour wind speeds. Richmond, Virginia had an earthquake in 2011, some five months after Fukoshima. It tripped generators as far away as Cleveland, Ohio. Not expected. Derechos … 200 miles wide, 600 miles long, 100 mile-an-hour wind [storms] that started in Chicago and ended in Washington, DC. Bombs planted in substations.

“I thought I’d seen everything, he said, “until Dr. Paul Stockton brought the EMP threat to my doorstep. And it reminded me of Randy Bachman’s song ‘You Ain’t Seen Nothing Yet.’”

Mr. Boston also strove to put this threat in context. “We’ve made a lot of progress, and the grid is not fragile.” PJM, he said, has seen a wide array of serious events in recent years. “And we know a lot about cybersecurity now. We had over 8,900 cases last November, a peak that was ten-times our normal average case load in one month. About 4,009 of those cases turned out to be verified threats trying to get through our firewalls, so it’s something that we know is getting worse and I expect it to get a lot worse before it gets awful.”

“But EMP,” he said, “is something I want to talk about today because it’s something that we have not had a lot of experience with.”

One could hope, he said, that some of the disruptive events in an EMP attack could cancel each other out. “My theory is that the nanosecond pulse that comes with the E1 will take out our relay and protection and control system. …Losing the system is not something I’m very proud of but in this case it could be a step towards goodness. Because the transformers aren’t damaged if

“ I thought I’d seen everything until Dr. Paul Stockton brought the EMP threat to my doorstep. And it reminded me of Randy Boxman’s song ‘You Ain’t Seen Nothing Yet.’"
they don’t overheat and overexcite. The generators have a better chance of surviving if they come down quick during an event.”

“I hope that theory is correct,” he said, “but I’m not willing to base the security of our country and our economy on that theory.”

“We need more than theories. We need test data. We need to be able to go to test facilities.”

Mr. Boston also spoke about protective measures worth examining. “When … I was working as a test engineer, we put two electronic relays and one electromechanical because we weren’t sure those new computers were going to do that well in the relay business. Today I suggest that we do the same, perhaps in the same relay cabinet.” As another example, “One thing I think we need that is key is our emergency generator sets [in our control centers].”

“In summary, we cannot redirect hurricanes. We cannot shoot down every incoming missile, even though the Department of Defense is good. We cannot stop every cyber attack. We can plan through. We can ride through. We can recover from severe events from man, and from extreme earth and space weather.”

“I define resilience very simply: … ‘It can take a lickin’ and keep on tickin’.’ That’s resilience. We talk about this a whole lot. It’s time for action.”

“We cannot redirect hurricanes. We cannot shoot down every incoming missile. We cannot stop every cyber attack. We can plan through. We can ride through. We can recover from severe events from man, and from extreme earth and space weather.”

“I define resilience very simply: ‘It can take a lickin’ and keep on tickin’.’ That’s resilience. We talk about this a whole lot. It’s time for action.”
Dr. Sanjay Bose, Vice President, Central Engineering, Consolidated Edison

The realities of running a power grid in a world with expanding hazards are quite different, Sanjay Bose pointed out, from the classroom environment. “I don’t remember any course that I took that would have allowed me to prepare myself for flooding or bullets coming into my transformer. I don’t know of any engineering course that teaches you how to design for [Hurricane Sandy].”

Mr. Bose summarized some of the flood mitigation efforts undertaken by ConEd after Sandy. “We put in 54 new concrete moats. … We put in 81 submersible 21,000 gallons per minute pumps. We sealed about 3,000 conduits. … We were given orders by a PUC to be ready by June 1st, 2013, … and if another Sandy [had come by June 1st] we would [have been] ready.”

ConEd, he said, has now protected to the FEMA-projected 100-year flood level, plus three feet. They have also invented “lifting relay panels” that can be cranked up, above flood level. “This has submersible connectors with fiber optics and communication cables, [since] one of the biggest damages we saw was getting water into copper. We decided we will change it to fiber, 80% fiber, so that will be EMP-proof.”

Con Ed has also invested in physical security. “And the objective was if we lose all the transformers in the substations how quickly can we … get the lights back? From Sandy we have learned that the maximum tolerance people can have is about three days without power. After that, no matter what happens or what caused it, people are not going to forgive you.”

As a result, he said, they developed plans for different contingencies. “If you lose all four transformers in that substation … you can take existing 345 volt overhead lines, run them at 138 with jumpers. We have the jumpers in the station. We’ve been doing transformer ballistic protection ourselves with the help of New York City Counter Terrorism groups.”
ConEd has also worked with a transformer manufacturer to develop a fully assembled EHV transformer designed to be transported, fully assembled and oil-filled. “It comes with its own radiator and oil cooler so there’s no assembly required. It’s self-powered, so feeds its own AC load. […] Transportable on a C-5, C-17, C-130, an AN-124, or an AN-225.”

In short, he said, “The orders that I’ve been given, … you have to get the entire loss of a substation restored in three days or less. It’s kind of tough. So we are in the process. I have orders now to order six of these.”

On financial impact, Mr. Bose said $1.8 is in the budget for storm hardening, planned for 2014 to 2017, system-wide. “And this is in addition to the billion-plus we spend each year on maintaining reliability. That’s not chump change!”

What does he foresee on EMP and IEMI? “We estimate about 5-6 million dollars per substations, but this is just an estimate. We are working with John Houston and folks to do that.”

Sanjay Bose concluded his remarks by making it clear they are looking for technical help in addressing emerging threats. “[For] our next steps, we need technical assistance. We want to understand ballistic protection, EMP protection. We are continuing to refine our recovery plans both from an engineering operation and emergency management perspective.”

And as a primary mechanism for such assistance, information sharing is key. “We also think we need a nation-specific strategic plan and an information-sharing model, which a lot of folks in here have talked about.”
Gerry Cauley focused his remarks on two hazards: Coordinated kinetic attack and GMD.

“What worries me the most is some sort of physical security attack on the grid. ... I was in the Corp of Engineers, combat engineer. I learned to blow stuff up, and shoot at things ... and if I could figure out how to ... put together a team and go out and disable, damage, and destroy equipment at multiple stations simultaneously and get away with it, I figure it’s something really we ought to worry about. That could ... have a very serious impact on the grid.”

As a recent example, Mr. Cauley referred back to the widely reported attack on the Metcalf substation. “This was not a lightly planned, frivolous activity. This was a very serious event. ... It suggests a change from everything that we had seen for 12 years.” Coordinated kinetic attack must be considered a serious hazard. “This tells us really the seriousness of considering a deliberate act to take down a portion of the power grid to affect our security or our wellbeing, or to inflict long-term damage.”

Gerry Cauley also spoke about GMD, and his view of the regulatory process for both GMD and physical security. “[For physical security] as well as in the GMD arena, we had an informed regulator, which I can point to because she’s here in the room. ... I think there was a bit of genius in both the GMD and the physical security orders in ... recognizing there’s going to be flexibility.”

Given the wide variability across the power grid, and regional differences in GMD sensitivity or considerations related to physical protection, flexibility was essential for both subjects. “The order allows that, and gave us the opportunity to essentially require critical assets to be identified, to do the risk assessment with outside third-party expertise to develop the security solutions, and to implement them under our oversight at NERC and FERC.”
CenterPoint Energy has been involved for some time in developing and implement protection against e-threats. In regard to GMD, John Houston expressed confidence that the existing process – especially the GMD Taskforce – will be key to addressing space weather concerns. “With regard particularly to GMD and the GMD taskforce, … I believe [their efforts] will result in our industry being able to address the mitigation of the solar effects on our systems.” However, he warned, it will be vital for power companies to understand how far they need to go to resolve the concern. “We don’t want to develop an action plan for the mitigation of geomagnetic disturbances and find out we have a disturbance as was described … this morning, and it doesn’t work. That would be basically an incrimination of everybody in this room.”

CenterPoint has also made a special effort to focus on EMP. “The EMP threat is one of those where we have to learn, project, and forecast what we need to do, and then do that in a way that actually takes this threat off the table.”

What has already been implemented at CenterPoint? “We have a new $170M control center under construction. About 8 million of that is for EMP protection to mitigate E1 effects on our control system computers.” The company has also developed their own EMP protected communication system. “As part of that project, [we are] installing completely redundant fiber optic communications to every substation, to enable resolution of any effect on our communication system from EMP, and to harden our communications systems from all our substations.”

John Houston also discussed the strategic motivation underlying CenterPoint’s investment. “Is this a real threat? I’ve been to four of these sessions and spoken at them, numerous discussions with many of the people in this room. I think it is a threat that we need to take off the table.”

“**We have a new EMP protected control center under construction. And we are installing completely redundant fiber optic EMP protected communications to every substation.**

“**EMP is a threat that we need to take off the table.**
There has been extensive reporting on the threat and, although substantial efforts continue to go into studying this hazard, work to broadly protect the U.S. power grid has not yet begun. “I’ve read the National Academy of Sciences and the EMP Commission Reports. … It isn’t for lack of people telling us it’s a real threat that it’s not resolved. I’ve been to meetings with DOD, DHS, FERC, the electric industry, EEI, and EPRI. … And we have a lot of work going on, in both the GMD and EMP arena, at EPRI.”

Part of the reason, John Houston said, is limited access to classified EMP-related information. “I’m trying to design a future substation that will have no EMP effects on its operation, and I’m trying to retrofit 280 substations … Those present unique challenges. But when I go to talk to … consultants who have done work for the military [and] I say I’d like to have the same kind of protection that is in a military base, [they say] we can’t talk to you about that threat level.”

DOD, he said, has a direct interest in making EMP information available to the power industry. “I think we heard our friends from the Department of Defense say they’re trying to prioritize their future priorities in terms of their mission. Now, their whole mission is to protect the United States and to be able to be a force for good in the event of some catastrophic thing like an E1 attack, an EMP attack. That mission may be compromised by our financial situation, but it’s totally compromised by the fact that 95% of their facilities require commercial power.”

To fully protect the grid against the EMP threat, he concluded, it will be essential that government share critical information with the owners and operators of the power grid that they depend on. “Until you bring me into the tent that says I’m just like your defense contractors, that I can have access to the EMP information and designs that are necessary to harden the facilities that are delivering your electricity, I cannot protect the grid.”
Rob Manning directed his remarks to the severe (terrestrial) weather hazard. “I have worked every hurricane you might imagine, many of the big names… I worked ice storms before they got names. I’ve worked a few after they got names.” Historically, he said, such hazards were addressed with a focus on reliability, redundancy and recovery.

“Now in those three R’s you won’t find resiliency … but I do want to say that recovery and redundancy I think have a lot to do with resiliency.” Nevertheless, he pointed out, lessons learned from the impact and recovery from Sandy have initiated major changes and improved resiliency. “There are huge changes not just happening at ConEd, but happening all around the country as a result of those lessons learned.”

Such improvements are important, he explained. Sandy is not unique, by any means. “I want to provide you with an example… It occurred in April of 2011 …the worst day for storms in the history of the TVA. Over that 24-hour period, we had three waves of thunderstorms come through our five-state area, but associated with those thunderstorms were 350 tornadoes. More than a year’s worth of normal tornados occurred in a 24-hour period. … five EF-5 tornados rated at greater than 200 miles an hour. It passed within four miles of the Browns Ferry nuclear plant … one of the largest in North America.”

The nuclear plant, Robert Manning said, was forced to operate on backup generators for a full week. Because of the magnitude of the outage, TVA had to exercise its black start plan. “We did a black start for the State of Mississippi, and a black start for the State of Alabama, and ran them as separate island systems for over a month before we were able to synchronize back to the grid.”
Mr. Manning went on to say that the bulk of the power restoration process was completed in seven days. It was their planning for redundancy that turned out to be critical, and looking forward, in any severe event, emergency communications will also be essential.

“There’s no problem that we can’t solve together,” he said, in conclusion. And referring to the full set of black sky hazards, “I’ve seen us solve problems before. We can solve these problems as well, and I think we’ve got a track record to prove it.”
David K. Owens, Executive Vice President, Business Operations, EEI

After flying all night, reaching the summit minutes before his presentation, David Owens opened his remarks by recalling his unique role during Superstorm Sandy. “I feel just like I did during Superstorm Sandy,” he said. “I feel exhausted and I feel exhilarated. When Superstorm Sandy hit the president wanted someone from the industry to go over to FEMA. All the storms that we had, this was the first time that they took someone from private industry.” He went on to talk about exhausting 19 hour days, and the exhilaration of “seeing just how our industry was able to mobilize.”

Sandy quickly became an important source of lessons learned. “I want to say a couple of things about that event, some lessons that have been learned, and then some gaps that I see from the conversation that we’ve had today.”

Mr. Owens started by reviewing the use of the power industry’s mutual assistance program in Superstorm Sandy.

“We mobilized … about 70,000 people.” With 28 states and 8.5 million people out of service, “We had to move crews from the west coast to the east coast,” he said, recalling the complexity of implementing this mass mobilization in real time.

“And then I met this gentleman named Paul Stockton who’s a real leader. The guy never slept, and I had the responsibility of working with Paul to try to mobilize these crews from the west coast, put bucket trucks in aircraft and move them … to the east coast.”

Government and industry worked together, he said, to make this process work in real time. For example, to expedite the process they needed waivers to run the crews through weigh stations and tollbooths. “That meant you had to work with the Department of Transportation. It meant also that you had to work with local government. Bill Bryan was helping out as well as other members of DOE.”

“When Superstorm Sandy hit the President wanted someone from the industry to go over to FEMA. All the storms that we had, this was the first time they took someone from private industry.

“We had to find places for people to stay. We had to find staging areas. So we approached the military …”
Lesson learned: Advance planning to support and expedite utility crews.

“A lesson to be learned is that as we look into the future, whether we have an EMP event, another natural response event, that we need to be able to expedite those crews.”

This will require coordinated, advance planning by government and industry. This became clear in Superstorm Sandy, when the logistics of managing the massive flow of people and equipment was complex. “We had to find places for people to stay. We had to find staging areas, where they could park their trucks, where they could live. So we approached the military about staying on bases.”

On the industry side, some new planning has already taken place, with changes made to re-plan the mutual response process for a national response event. “Now we have a mechanism where we can allocate crews nationally if we have an event that transcends more than one state, and results in a major disruption of electric service to customers.”

Lesson learned: Advance planning for utilities to use DOD Facilities.

We need an agreement with DOD facilities that if we have a major event in the future, that we would be able to use military facilities.

Lesson learned: Modify the Stafford Act.

Another consideration, based on the experience of Superstorm Sandy, is to consider revisions to the Stafford Act that could speed and improve the process of providing federal aid in a major disaster, including to utilities, which will be critical in any major disaster. “If we’re going to do something in the future where we see a major natural event we’ve got to do something about this Stafford Act.” This is a gap, he said, and it will be a problem for EMP, cybersecurity, or any other national response event.

And then I met this gentleman named Paul Stockton who’s a real leader. [We worked together] to mobilize these crews from the west coast, put bucket trucks in aircraft and move them to the east coast.
Lesson learned: Staged inventory of critical spares.

On assuring the availability of critical equipment. “When we talk about EMP or any of these other [events], we’re looking at critical infrastructure equipment, [such as] transformers.” How should this be addressed? Mr. Owens proposed that there needs to be both a designated supply of critical spares, along with a comprehensive inventory so the components and their locations are known, and can be used effectively.

“We need to have an arsenal of spare parts equipment. We need to know what the government has. We need to have an inventory of what we have if we’re going to have an intrusion. Irrespective of what the event is, something that had a significant impact on society, we need to know where those facilities are.

Lesson Learned: Contingency planning for transportation of heavy equipment.

“We need to be able to move those heavy-duty, 90,000 pound transformers … from one area to another. That’s a gap. We don’t have a roadmap to do that.”

Lesson learned: Emergency Communication

“The other gap that I see is … private communication. Cell towers were down … We need to find a way where we have clear-cut communication if we have an interruption. We also need to do something else. We need to realize that our chief information officers have a vital role here.”

Lesson Learned: Tools and technologies

Referring back to a point made earlier by John Houston, David Owens emphasized that as an important need. “We need to be able to have prevention, and those are the tools. And we have a gap here, folks. … We really need to be very focused on the kinds of tools that we need. That we can in fact deal with EMP events, we can deal with physical events, and we can deal with cybersecurity events. …We need to enhance [the government / industry] dialog where there’s some sharing of these tools and technologies.

Lesson Learned: Training and exercises

“We’re all about preparation,” he said, praising Gerry Cauley for GridEx2. “That means we’ve got to do drills. We’ve done drills with the government. I compliment Gerry on GridEx II.”

Lesson Learned: Funding as an enabler for response and recovery

David Owens concluded his remarks by referring to two gaps: cost recovery for resilience investments, and Stafford Act limitations on federal funding for utilities in an emergency. “We need to improve our response…. And the recovery is very expensive to do the things we talked about today. So there’s cost recovery and there’s also the recovery of acknowledging that the Stafford Act is an issue. I think those are gap areas.”
Session Four

Multi-Sector Planning for Black Sky Days

Introduction: Grid Continuity Planning in Two Dimensions - Multi-Infrastructure Resilience, Cross-Sector Response
Introduction

Dr. Paul Stockton introduced the Session topic – Multi-Sector Planning for Black Sky Days – by challenging the delegates to help develop approaches to prepare for black sky hazards. “How can we support industry for power restoration,” he asked? “How can we simultaneously limit the consequences of large-scale, long-duration power outages for societal continuity; for the threats to public health, public safety, national economy, and national security that a long-duration outage might cause?”

This goal, he pointed out, is unachievable, “unless we’re able to partner together, and plan in advance to both speed power restoration, provide industry with the support it needs, and also deal with consequence management challenges that will be unprecedented in American history.”
Dr. Paul Stockton, former U.S. Assistant Secretary of Defense, Editor-in-Chief, EPRO Electric Infrastructure Protection Handbook

The EPRO Handbook: A decision support tool, hosting opportunities for concrete progress

The Electric Infrastructure Protection Handbook, he said, is being developed as a framework – a decision support tool – to host this planning process. “I believed when I was in office, and I continue to believe today that there is not a go-to document that brings together, that fills the gaps between all of the activities that are going to be necessary in order to build resilience against these non-traditional hazards to the electric power grid.” The Handbook, both the first volume now in development and future volumes, are designed to help fill that gap.

“There are many cylinders of excellence … The challenge is bringing these different components of the overall resilience system together,” he explained, “all of the stakeholders … who are going to be required to build practical solutions to the resilience challenges we confront.”

“All of these perspectives need to be brought together in a way that’s useful for decision makers, not any kind of prescriptive one-size-fits-all approach.” And it will be important, he said, to include international perspectives.

The Handbook framework should also act as a decision support tool, a consensus document helping to frame the challenges, and host “emerging best practices, opportunities for concrete progress.”

The EPRO Executive Steering Committee (EPRO ESC): Supporting implementation of consensus measures

“In addition to putting out the handbook to serve as a decision support tool, we are going to stand up an Executive Steering Committee, because clearly the implementation of these recommendations going forward is what we really care about. We’re not interested in just producing a beautiful document.” The focus

“Why the EPRO Handbook?
There is no go-to document that fills the gaps between all of the activities necessary to build resilience against these non-traditional hazards to the electric power grid.

“There are many cylinders of excellence … The challenge is bringing these different components of the overall resilience system together,
of EPRO ESC is to help utilities and their partners to strengthen resilience against these severe hazards. “What we want to do is strengthen resilience in measureable, significant ways that reflect the need for industry and all the other partners to be able to manage risk in a way that’s going to work for them.”

This challenge, he pointed out, will be to find ways to use a cross-sector, collaborative approach to help agencies, governments and corporations make progress, together, in ways that are not achievable on their own, while still reflecting their own unique priorities. “So to provide for a collaborative framework, and sustained progress both in implementation and dealing with the many resilience issues that are going to remain, that’s going to be the purpose of the steering committee. And we’ll want representation from all of the partners in this room today.”

Moving beyond protection

There are two critical objectives, Dr. Stockton explained, for the response effort to a long duration, large regional power outage:

“First of all, support for power restoration,” which is fundamental to any successful recovery.

“Then secondly, deal with the threats to public health and safety that are going to emerge in these kinds of black-sky events. We’re going to face twin challenges, very closely related problems,” he said, “that are unsolved today. Progress is underway but we aren’t where we need to be.”

How do cross-sector requirements come into play? “There are going to be enormous requirements for life-saving and life-sustaining operations, on the part of government, non-governmental organizations, and faith-based organizations.” FEMA, state and

“In addition to putting out the handbook to serve as a decision support tool, we are going to stand up an Executive Steering Committee, because clearly the implementation of these recommendations going forward is what we really care about.

“The environment in which we’re going to have to operate in order to save lives is itself going to be severely disrupted.”
local agencies, public safety officers and the Department of Defense, among many others, will be heavily involved.

Beyond power, there will be a range of critical services and resources that will need to be sustained at some level, and quickly restored. “Absence of water, disruption of wastewater treatment, these are problems that immediately are going to pose immense challenges. […] If you look at the major urban areas in the United States, [almost] every one of them … depends on electricity for that municipal water system to function.”

Other critical requirements: “Transportation, communications, hospital functioning, food distribution….” All of these are fundamental to the health and continuity of modern societies, and in an extended power outage, all will be seriously affected. “The environment in which we’re going to have to operate in order to save lives is itself going to be severely disrupted,” he pointed out. And government and NGO emergency responders’ effectiveness depends critically on the availability of these same resources. “That’s the paradox. There’s a huge demand for life-saving activities but the ability of the organizations to provide that capability is itself going to be severely compromised.”

And in addition to these normal, day-to-day resources and utilities, there is a critical issue with another resource, a vital resource spanning all aspects of society that only comes into play during a power outage: Emergency Power.

“I want to refocus on the challenge of emergency power: […] In a long duration outage, the mismatch between the demand for fuel and the resupply of generators as they burn out, the demand for those emergency power components versus the supply, that is a catastrophic gap that we have no plans currently to manage, none, except in some very specialized areas of the Department of Defense.”

**Where do we need to go?**

In summary, he said, “We need to begin tackling these challenges of not only how are we going to meet the overwhelming demand for life-saving and life-sustaining capabilities but to do so in an environment that’s severely disrupted.” Saving and sustaining lives in this environment, while also helping support utilities’ power restoration efforts will require a wide partnership, including government and non-governmental organizations, the National Guard, law enforcement and a wide range of other stakeholders, all with missions far larger than have been seen in previous disasters.

“It’s a solvable problem,” he said, concluding.

“But we need to begin identifying the gaps today, planning for them, and exercising these plans. If you don’t exercise it, it’s not real.” And in fact, he said, “Immense progress is being made. … I think there are best practices going forward now in the aftermath of Sandy.” The Department of Energy, FEMA, the States, the Department of Defense have all captured lessons learned after Sandy, and have important initiatives under way. “What we’re missing is an effective means of sharing these lessons, and especially across sectors. We need the handbook to do that.”
Gerry Cauley, Dr. David Elmakis, Dr. Trevor Gaunt, Frank Koza and Raj Rana provided perspectives on the role of the electric sector on multi-sector planning for black sky days.

One message, coming from all panelists, was that this train has left the station. Work has been going on, and is expanding, to address the potential for a major, national-scale power outage. This has included, for example, a major exercise looking at malicious attacks on the North American bulk power system. While important progress has been made, it was clear that most of the effort to address these uniquely serious hazards remains ahead of us.

One challenge highlighted was closely tied with similar observations coming from many panels: After an event, “unity of effort” will be essential, with a well-coordinated process that involves the utility owners and operators, and the various relevant government levels and agencies. It will also require another dimension: pre-event investment, such as wide industry involvement in incremental resilience measures against electromagnetic threats and other black sky hazards. In this area, Dr. David Elmakis gave a number of specific EMP-related examples, not included in this report due to security considerations.

In addition, access to appropriately inventoried and staged spares was identified as a related concern, with hardware assets spanning many companies, locations and jurisdictions.

Some aspects of severe space weather were discussed by the panel, including considerations related to the nature of an extreme event. High GIC levels, for example, may not be the most important stressing event, it was suggested. There is evidence to suggest that a very long duration, much lower level GIC event could create a more gradual but very extensive problem, which must be considered by those looking for best practice protection of critical EHV transformers and other high voltage equipment.

Panelists also discussed their participation in the EPRO Handbook, anticipated to be a unique resource for power companies and other stakeholders. While the Handbook speaks to incremental, cost effective E-threat protection measures and all hazard, whole community response, panelists pointed out that priorities during the actual recovery process would operate from a completely different economic perspective, essentially setting aside optimal economic factors until the grid returns to near normal conditions.
Dr. David Elmakis, Senior Vice President, Planning, Development & Technology, Israel Electric Corporation

Dr. Elmakis spoke of historic and ongoing work by Israel Electric Corporation to protect against both Severe Space Weather and EMP. His presentation is restricted.
Framing work going on to address black sky hazards in the electric sector, Gerry Cauley focused his presentation on GridEx2, a large scale power outage exercise conducted in North America, the United States and Canada, and a portion of Mexico.

Why an exercise? “Unless we exercise [our preparations] and unless we test them and challenge ourselves, it’s not really going to work effectively.”

The challenge for GridEx2 was a combined physical and cyber attack, as an example of a stressing scenario. How stressing? “We had the support of both industry and government to essentially overwhelm the system, overwhelm our capabilities, and see what opportunities we had to learn from that.” Among the lessons learned – in such a scenario, even understanding the scope of the problem can be challenging. “There was a lot of confusion about what data could be relied on … But we did find that companies had a lot of emergency plans in place that worked.”

**Lesson learned:** The need for unity of effort in a national-scale event

Among the major lessons learned, one was the impact of the scale of the event, and the consequent need for “unity of effort.”

“This is huge,” Mr. Cauley said, “and I don’t know how we would respond to this. So we have agencies and we have industry plans but we’re … not really looking at a major, major national disaster. […] How do we pool our resources together and implement our plan, so plans are not really just paper documents? How do we turn this into reality?”

“But how do we make sure everybody’s working together for the same purpose?” In other words,
for a truly massive event, real time organization and optimization of resources, while difficult, will be essential. “The unity of effort challenge was very difficult because everyone wanted to deploy their resources for their purpose, but how do you coordinate those?” he asked. “There’s a whole set of issues that need to be dealt with, [especially] getting somebody in charge.”

**Lesson learned:** Grid restoration needs to be a key priority for security providers

A second lesson learned was the importance of law enforcement and security. “With active shooters, explosions, [and] recognition immediately of a national emergency, law enforcement [will be] making sure that the people are safe. It may not be a priority to secure and escort first responders from the power company or other first responders.” The consequences could be serious for restoration. “The early response from the utility CEOs: ‘I’m not going to send my people into a dangerous zone until I know that areas are secure.’”

**Lesson learned:** Dependable, well-communicated situational awareness is vital

“How do we get the replacement breakers and equipment, the spare transformers? And how do we get those together quickly and deployed?”

**Lesson learned:** The importance of the supply chain. Pre-planned, accessible supplies

In any major event, the normal process for locating, acquiring and transporting critical equipment breaks down. Spares likely to be important in national scale, black sky hazards would need to be pre-deployed, with accessible inventory information.

“The final [lesson learned] was in the area of supply chain. If you’re looking at damage to equipment and outages a month in … how do we get the replacement breakers and equipment, the spare transformers? And how do we get those together quickly and deployed to have the recovery?”
Dr. Trevor Gaunt, Professor, Department of Electrical Engineering, University of Capetown, South Africa

During and following the “Halloween solar storm” in the fall of 2003, South Africa’s ESKOM saw the failure of a number of their high voltage transformers. Dr. Trevor Gaunt, who has studied these and related Geomagnetically Induced Current (GIC) events, spoke about the impact of such events on high voltage power grid components.

While there have been improvements in our understanding of solar weather, forecasting severe solar weather events, and their impact, remains beyond our capabilities today.

Another issue, he said, is understanding the GIC sensitivity of Extra High Voltage (EHV) transformers. “[They] are poorly understood. Generally when they’re happy they sit there and hum, and you know they’re unhappy when they growl at you,” he said. “But what’s actually happening there, and which transformers are prone to damage is a matter of great dispute within the industry. It’s actually worse than that because what the effect is on the power system is generally unknown. The models, the standard definitions of reactive power and harmonics, and how the network responds are very simplistic,” he said.

What does this mean for the vulnerability of specific transformers? “The mechanisms of degradation and failure of transformers are also in dispute,” he said, pointing out that “most utilities don’t even monitor the condition of their EHV transformers, except that they take results of dissolved gas analysis and file it. They forget to interpret it.”

Work is also needed on mitigation, he argued, since “the efficiency, the effectiveness of alternative mitigations have been really untested … and in terms of having redundancy, nobody values redundancy until it’s needed.”

Dr. Gaunt concluded his remarks by suggesting that the most dangerous solar storms may not, in fact, be those with the highest intensity. “What do you think is the worst storm event that we

“Some officials hope in an extreme event you’ll lose the network and all the equipment will be protected. But imagine that in a probability distribution, if the event is not that severe but it’s a long duration, all your transformers will be well grilled. They’ll be like overdone steak. Not nice.
should be considering? My suggestion is that it’s not an extreme event in intensity, but a long-duration event. “The Carrington Event lasted 6 hours. The Halloween Storm lasted 5 days.”

Why? Some industry officials hope that “in an extreme event you’ll lose the network and all the equipment will be protected. But imagine that in a probability distribution, if the event is not that severe but it’s a long duration, all your transformers will be well grilled. They’ll be like overdone steak. Not nice.” And therefore, he said, “sometimes we’re looking at the wrong kind of mitigation.”
“Last week, FERC approved the first [GMD] standard, and basically the standard will require that every transmission operator in North America develop an operating procedure to deal with GMD.”

“This is not going to be one-size-fits-all kind of situation,” he said. However, “each transmission operator will now be required to develop an operating procedure to deal with GMD. The second standard … will require each of the planning authorities in North America to conduct a vulnerability assessment of their transmission system.”

While there may be different opinions of the best benchmark for the first time, in North America, “it will require everybody to have that capability and to conduct the analysis. … if you cannot meet the requirements of the benchmark, the standards will require that you develop a corrective action.”

Frank Koza also referred to the EPRO Handbook, which includes material reviewing different approaches for GIC mitigation. “I’ve been fortunate to work with Paul and the EIS team in helping to develop the handbook,” he said. “I’m going to try to continue to support it. I think it will be a valuable tool for use by the industry.”

His role in that development, he said, is largely derived from his operational experience. “What I try to bring to the table is kind of operational perspective on GMD events, and EMP.”

This can be important, since mitigation measures need to be understood in an economic context. “We’re trying to … extract the maximum economic benefit out of that set of facilities.” Embedded mitigation measures could mean compromising, to some degree, a grid configuration that has been optimized for the non-black sky environment.

“So when you look at these kind of severe events … any kind of response will mean we’re going to sacrifice the economics of the system to be able to save it in the course of the event. … to be able to save the power system, to come back from these kind of events.”
Raj Rana, Former Director - RTO Policy and NERC Compliance, AEP

In characterizing the differences between the consequences of an EMP event and a typical, historic power outages, “you’re going to have a lot of failures or damage to the electronic equipment, and some of the major long-lead items, such as power transformers, and even generators.”

The key consideration, Raj Rana said, is minimizing restoration time, and that requires three key elements: “At a minimum, you need to increase the resiliency or the hardening of some of the major equipment and electronics that you’ll need as a part of the restoration process.” This would include black-start power plants and associated cranking paths, which can then be used to restart other power plants. And protecting enough control centers to maintain access and control over the grid will also be important, to guide the restoration process. Appropriate, pre-staged spares, he said, would also be part of this process, as well as appropriate tooling and diagnostics.

For this to be effective, however, power companies will also need to have “a flexible, adaptable restoration plan” designed for such an event.

The third element, he explained, is external support to the power industry’s restoration process. “Considering that it’s over the very large geographic area … you need to have collaboration between the electrical sector, along with the public sector, which would include your government agencies, as well as NGOs, non-governmental organizations.”

Summarizing preparation strategies, he referred to a range of choices for system hardening levels: “At minimum,” he said, “what you can do is to harden or increase the resiliency of components that are involved as a part of the system restoration.”

“Considering the very large geographic area, you need collaboration with the public sector, which would include government agencies and NGOs.

“At minimum, what you can do is to harden or increase the resiliency of components involved in system restoration.
Overall, the process of defining what equipment to protect will be different for different grid segments, and will depend on the level of hardening selected in each case. This could include, for example, “selected transformers, critical black-start power plant GSUs, electronics at critical substations along the critical cranking paths.”

Mr. Rana also emphasized the importance of assured emergency power. “Backup power [will be essential] for stations critical to system restoration, including selected black-start power plants, substations on protected cranking paths, and a control center.”
Miles Keogh, Thomas MacLellan, and Jonathon Monken spoke of Black Sky hazard planning from the perspectives of State and local government.

States have primary responsibility for emergency response, and in the post-Sandy environment, with energy assurance now a primary concern, the need to prepare for long duration outages has also become a subject of interest to governors. And given the complexities expected for emergency response to such events, advance preparation must include pre-planned prioritization of critical assets.

Repeating a theme that came up repeatedly in the summit, this panel highlighted unity of government as a critical need. Government coordination at all levels will be essential, including private utility owners and operators, NGOs and other stakeholders. In the highly disrupted environment following a major earthquake or some other black sky hazard, recovery will only be possible with well defined, pre-planned leadership that has access to all relevant interconnected public and private assets and organizations. And this coordinated leadership process must address both the federal-state interface, and the needs for seamless recovery operation across state and jurisdictional boundaries.

This complex process cannot be invented in real time – it must be developed in advance, and made effective through extensive training and exercises.

From a regulatory perspective, in today’s environment, such planning faces significant challenges. Coordination among agencies is typically difficult. As one consequence of this, at the highest level, while an understanding of the need to address severe hazards is usually associated with threat expertise, such expertise has typically not been accessible to regulators. This problem is exacerbated by structural problems, since the metrics normally used to evaluate resilience investments are not designed for major outages.

And a message that echoed throughout the summit was articulated clearly by this panel. Preparing and planning for recovery from black sky hazards cannot be a “business as usual” subject. Those entrusted with supporting this effort have a human responsibility that transcends the normal bureaucratic process.
Miles Keogh, Director of Grants and Research, National Regulatory Commissioners Association, (NARUC)

From the perspective of utility commissions, the key is to find a balanced approach to “enable utilities to make investments in resilience, in infrastructure, and in human infrastructure that helps avoid or get us through the worst kinds of events.”

One of the keys to this process is effective communication to commissions, and exercises can be a particularly effective tool. “If you want to really teach somebody something, what does work in fact is play,” Miles Keogh said. “It’s games. It’s interactivity; it’s putting your hands on things.” NARUC has made that a focus of their programming. “My colleagues and I at NARUC have really tried to focus on using games, interactive sessions and scenarios, exercises, and the like to put new information in the hands of the commissioners and the commission staff in a way that really works.”

As one example, Miles Keogh and his staff worked with EIS Council to put together an exercise focusing on a black sky hazard, “where we would allow folks to kind of come into contact with information about the implications of a very large-scale, very long-term failure of the electric power infrastructure.”

Representatives from FERC, DOE, ConEd, PSE&G and others participated in the exercise, in which a rogue element detonated a high-altitude nuclear weapon off the coast of a fictional city called Gotham. “What we really wanted to do is look at the decision-making processes that underlie how we make decisions about long-term investments or about investments that help deal with catastrophic kinds of events.” Resilience investments for severe events compete with investments in day-to-day reliability. “One of the things we discovered is that in that kind of scenario … you just can’t provide the services if the infrastructure fails, to about 20-30 million people. They need to pack up and go spend the winter in refugee camps in other parts of the country where the infrastructure is still working.”

From the “Gotham” exercise, three major “lessons learned” were identified: systemic problems leading to serious policy issues.

“…The folks who are in the business of identifying the threats and managing the risks tend to be in a completely different stovepipe than the folks who are approving those investments.”
**Lesson learned:** Threat and risk expertise is generally not accessible to those controlling the investment that could buy down that risk

“The folks who are in the business of identifying the threats tend to be in a completely different stovepipe than the folks who are approving those investments.”

**Lesson learned:** Utility cost effectiveness metrics systematically undervalue investments critical to survive major outages.

“The second, and maybe this is the most pernicious of the three things we’ve found, was that the way that we evaluate the worth-itness of investments tends to systematically underprice investments that avoid or mitigate or deal with long-term outages.”

Frameworks used to evaluate the value of investments are optimized for the business as usual environment. “One of [these frameworks], for example, SAIDE – the System Average Interruption Duration Index – … addresses how long an outage is.”

In other words, “expensive but rarely used kinds of investments, ones that deal with low probability but very high consequence investments are still an extraordinary tough sell, even if you tell people that the punch is coming.”

**Lesson learned:** Breaking the stovepipes is difficult, even when essential to recovery from a severe outage.

“The third thing is that systematically it is very difficult to arrange working together. A lot of the things that governments do well they do well because we set up natural tensions between agencies that represent opposed or competing interests. And generally that’s good,” Mr. Keogh pointed out. But in a severe emergency, these competitive structures can be problematic. “And that problem also … increases exponentially when we get out of the United States.”

“Maybe the most pernicious of the three things we’ve found: the way we evaluate the worth-itness of investments systematically underprices investments that avoid or mitigate long-term outages.”

“[While broad coordination is essential for recovery from a major disaster,] “Systematically, it is very difficult to arrange working together among agencies that represent competing interests.”
Thomas MacLellan, Director, Homeland Security & Public Safety Division, National Governors’ Association

“It’s not going to be the president who’s going to be responding to the disasters. It’s going to be the governors of the states.” This means, Thomas MacLellan pointed out, that governors are the primary focus in preparing for recovery from a major power outage.

Thomas MacLellan opened his remarks with a reminder of the importance of the subject of the summit given the scope of what a severe black sky outage would mean for the population, people involved in preparing for such a scenario need to have well-founded priorities that go far beyond “business as usual.” In that regard, he quoted the famous words Sir Thomas More, who said, “I am the King’s good servant, but God’s first.”

But beyond such global perspectives, what are the critical messages for governors?

“I run what’s called the Governors Homeland Security Advisors Council,” he said. And the reality is that, before a disaster, preparation is unpopular. “The message that we give to governors around disasters and preparedness and response is that disaster response, Homeland Security is not going to get you elected. But it will,” he continued, “tie up your agenda, or it will get you unelected in a subsequent election. And that helps get their attention.”

What examples does he use? “When I talk to governors,” he said, “and I start talking about energy assurance, the lesson I say is: ‘Fukushima wasn’t an earthquake. Fukushima wasn’t the tsunami. Fukushima happened because it was a power outage.’”

Given their role, the primary focus for governors is emergency response, he explained, not protection. “There are some response and preparedness issues that probably will pertain to what the threat vector ultimately is: EMP, cyber, kinetic, something like that. [...] But what we care about really for governors at this point is response.”

“Addressing threats of this magnitude cannot be in a business as usual mode. As Sir Thomas More said, “I am the King’s good servant, but God’s first.”

“The message we give to governors is that disaster response will not get you elected. But it could get you unelected.
NGA is involved in a number of initiatives to build recovery planning at the state level. One such initiative was kicked off earlier in the year, addressing black sky power outages, “This March, … we hosted … a workshop on a massive and prolonged grid failure and what’s the role of governors.” With EIS Council’s participation, the workshop helped open a window into a hazard level that is not well understood. “It was a fascinating and often frightening discussion … In some respects it’s an existential threat.” The workshop, and the detailed discussion that took place among the many participating state and federal agencies, was also an important resource in developing the EPRO Handbook.

Workshop participants broadly agreed that prioritization of resources will be a critical issue. “There will be winners and losers, and you have to have those discussions first, and you have to have them honestly. Hospitals may not be the winner.”

“Those discussions need to happen,” he said. “They need to happen in advance.”

Power restoration planning is another example. “Restoration planning needs to be included in every discussion that’s taking place within the Homeland Security apparatus in states right now for power.”

The good news, he concluded, is that in the post-Sandy world, governors now understand that energy assurance is critical. Referring to a recent meeting with more than 25 governors, “Energy assurance was one of their number one issues,” he said. And they understand preparation has to go far beyond paper plans. “One of the notions that governors are beginning to get is train, train, train. Know your plans, train to your plans.”

“**We hosted a workshop on a massive and prolonged grid failure and the role of governors. It was a fascinating and often frightening discussion … In some respects it’s an existential threat.**

“**There will be winners and losers, and you have to have those discussions in advance. Hospitals may not be the winner.**

“**Power restoration planning needs to be included in every discussion on power taking place within the Homeland Security apparatus in states.**
Jonathon E. Monken, Director of Illinois Emergency Management Agency (IEMA); Chairman, Central United States Earthquake Consortium (CUSEC)

“We have a collective responsibility to really execute this response, and the challenge that we have in trying to communicate what we’ve discussed here, not just internally with the subject-matter experts, the believers if you will, but really the folks that are not familiar with what we’re talking about.”

The key to making progress, Jonathon Monken said, is to communicate to decision makers the scope and urgency of addressing national scale power outages. But that, he pointed out, is not enough. “One of the biggest challenges we face, is … to coordinate [response]. Especially if you’re trying to coordinate it after the fact. If we don’t demonstrate a unity of government, we cannot possibly have a unity of effort.”

The coordinated response that will be essential in disasters of this scale can only be achieved, he explained, with pre-planned, broadly coordinated government action at all levels. “Unity of government is a very difficult thing to achieve. But it’s something that we have to place in front of us, knowing that it is our responsibility, in a no-fail contract, with the citizens of our respective countries, that we will be there. There is no such thing as a circumstance where you say wow, that was a really bad one, and you know what, it’s just too big, I’m sorry, we’re not coming to help you. We don’t have that luxury.”

How can we make progress toward this goal, with a well-coordinated effort that brings in all the stakeholders? “Well, I think then it comes down to trying to understand the importance of catastrophic-level planning and exercise. […] If you can plan to that level, everything else is gravy.”

Jonathon Monken spoke of a recent example, with state emergency management agencies, utilities and other stakeholders working together in an exercise simulating a massive earthquake in the New Madrid Seismic Zone in the southern and Midwestern United States. “The New
Madrid CAPSTONE 14 exercise was the first time we’ve ever executed concurrent exercises with the private sector as a result of over two-and-a-half years of planning.”

In a disaster of this magnitude, he explained, with urgent needs greatly outstripping available resources, coordination and prioritization will be particularly critical. “What it comes down to, when we got into the exercise … is the joint prioritization with the private sector.”

“What happens when there are not enough line trucks in the country to handle the problem that you’re facing right now? What’s the point of getting the power turned back on to the hospital; if it doesn’t have water connectivity you can’t get fresh water to it. The roads are blocked so you can’t get an ambulance there, and the communications are still down. So nobody even knows which hospital’s functioning right now. You can’t even dispatch your services.”

In sum, the coordination and prioritization challenges will be enormous. And, at all levels, the challenges reflect the interdependence of infrastructures, and the critical role of electricity. “The interconnectivity of all of these systems has a nexus with electricity and power.” However, in the current reality, power companies simply work to their own restoration priorities. As one power company official told him, “We have our own system of prioritization.”

However, in a severely disrupted environment, a power company-exclusive prioritization process will not be workable, with power companies themselves now dependent on external information and resources. “So trying to have that give and take in a very operational sense is very important, and it draws out some of the lessons … there are services that need to work collaboratively to execute their missions.”

An overarching issue in a disaster of this scale is the need to think and plan for resilience and

“**It comes down to the importance of catastrophic-level planning and exercise. If you can plan to that level, everything else is gravy.**

“**What happens when you have a multi-state response? How do you deconflict those resources?**
response strategically, especially in balancing and allocating state and federal resources. “But the hard part is the policy framework and the legal framework that exists says that only FEMA, that’s the only authority of the federal government that has the legal authority to adjudicate resources.”

“At the state level, that resides with the governor. But what happens when you have a multi-state response? What happens when state mutual aid kicks in? How do you deconflict those resources?”

Based on the Capstone 14 experience, this is a far from abstract issue. “Just the first 72 hours required 26 states’ worth of assets. And we hadn’t touched the federal government yet.”

And this need for broad coordination and prioritization, including all levels of government in addition to power companies and other critical stakeholders, has far too many dimensions to be addressed without thorough advance planning.

Mr. Monken used fuel logistics as an example, based on the Capstone 14 exercise: “Don’t worry,” we were told, “DOD will provide it.” In fact, however, “sixteen entities have MOUs with the same airport to use it as a base of operations in that scenario. Anybody else think that might be a problem when everyone shows up at the same time?” On this in particular, he said, “there is an important discussion to have here to talk about the concept of what I would refer to as a common-user logistics system,” including inventory, availability and distribution of everything from fuel to food and fresh water.

“How do we integrate these systems in a meaningful way to make sure that one, we’re not duplicating effort; two, we’re not wasting anything; and three, we have enough to prioritize as we go through.”

“The important thing,” he concluded, “is that there’s a plan. If the plan doesn’t exist before we get to it, there’s no way to effectively communicate it when it happens. And that’s how panic is induced in a large society experiencing a catastrophic event with long duration.”
Deputy Assistant Secretary Bill Bryan, Assistant Secretary Caitlin Durkovich and Assistant Secretary Todd Rosenblum and Director Joseph Shapiro spoke of some of the roles of federal departments and agencies in planning for black sky hazards. Support to private industry and the owners and operators of utilities is a well-recognized, important priority, and this includes information sharing and other means that government agencies can use to support infrastructure resilience. This includes support from the Department of Defense, which can bring significant resources to help in response to major disasters, in support of FEMA.

Within DHS, FEMA has a central role in coordinating federal support to the states’ emergency response efforts, and for other recovery support efforts.

In this panel, homeland security perspectives addressing Israel’s needs highlighted EMP as an example of a severe, high impact threat that are being seriously addressed, including work to include EMP in a formal “Reference Threat” document that helps activate government-wide response. In addressing such threats, statistical, probability-based assessments are not considered relevant, and must be replaced by expert threat analysis accounting for a number of strategic factors.
In speaking of the role of DHS in addressing a severe, long duration power outage, Assistant Secretary Caitlin Durkovich added another dimension to the comments, by many speakers, of the importance of broad coordination.

“The Department of Homeland Security is very committed to working with owners and operators, to ensure the security of our electric grid. And again, we do this in partnership with our federal partners, certainly with state and local government, and in support of owners and operators.”

Overall, the Assistant Secretary pointed out, the many aspects of government engagement in a disaster are mediated by a common framework. The National Response Framework sets the stage for how we come together as government and industry to respond to these incidents,” she said.

One important element of this effort is information sharing, particularly on threats that relate to utilities. “Our job at the Department of Homeland Security is to help owners and operators understand the risk. And again, give them the tools to mitigate it.”

Given the wide range of risks addressed, DHS prepares for many different scenarios, making use of synergy, where possible, to help expand their effectiveness. Information sharing can be important to assure resilience resources are invested wisely. “But at the end of the day, we’ve got limited resources, and it’s incumbent on us to help industry make wise investments, and for us to do the same.”
Deputy Assistant Secretary Bill Bryan opened his remarks speaking of resilience, using an example from Hurricane Katrina to showcase the flexibility and resilience of private industry. Private industry, he pointed out, is key to resilience against any severe disaster. “The people, asset owners and operators are the ones that own … resilience. They own it and they’re the ones ultimately responsible to carry it out, but we as a government ought to be able to enable those kind of activities to go on.”

DOE’s role in power outages, Mr. Bryan explained, is framed by Emergency Support Function 12. Within DOE, his role spans three different domains, addressing reliability, survivability and recovery. And within those three domains, “I focus on both the infrastructure security side of things, as well as energy restoration.”

How does this take place? “The Electric Sector Coordinating Council is represented by CEOs,” he explained. Their direct involvement has a substantial impact “on the way the electric industry responds to disasters in the United States, and responds to threats, all threats, not just natural disasters, but all threats.”

Addressing oil and gas issues, however, can be more complex. DOE works with the National Petroleum Council. However, with antitrust issues and other considerations, he explained, it is far more difficult to get coordination across the oil and gas sector. “And during an event, we have to work with them very differently.”

The key, however, is to work to help enhance and enable the resilience of utility owners and operators. “However you define resilience, we don’t own it, but we have to enable it.”
DOD’s involvement in recovery from a disaster exists within carefully described legal boundaries. “When we do defense support of civil authorities, we work for FEMA. We report and support FEMA. We take our mission assignments from FEMA,” Acting Assistant Secretary Todd Rosenblum explained.

DOD, therefore, acts in a support role for such events, accepting, rather than defining, missions. “In DOD, we need to have a very clear understanding of what the expectation is, when an event is going to be big enough, large enough that the normal response efforts are likely going to be overwhelmed.”

What are typical roles? “Most often, our support plays to DOD strengths: lift, logistics, the ability to move quickly, the ability to have communications, the ability to bring just mass to a problem.”

In fact, however, Assistant Secretary Rosenblum pointed out that one of the most important capabilities DOD brings to the table in a disaster has not been well understood. “The really impressive capability that DOD provided to Sandy support was frankly our ability to let contracts faster than anyone else in the federal government.” For example, “We didn’t own any of the generators that were brought in. We owned the capability to do contracting immediately. And we got that assignment again from FEMA.”

DOD’s capabilities in disaster response, while substantial, are not built in as a primary function. “The Department of Defense is neither authorized nor appropriated to build capability for the purposes of domestic response to state events. It’s a dual benefit … that’s provided as long as the Secretary of Defense can say it is not impacting the readiness of the Department of Defense to execute its military responsibilities.”

“**When we do defense support of civil authorities, we work for FEMA. We report and support FEMA. We take our mission assignments from FEMA.**

“**Most often, our support plays to DOD strengths: lift, logistics, the ability to move quickly, the ability to have communications, the ability to bring just mass to a problem.**
Nevertheless, when called upon, DOD’s capabilities are substantial. “We have capabilities resident all over the United States at our defense installations. There are rule sets and authorities by which we have community partnerships … Our installation commanders, they have compacts with local communities in which they can provide that immediate response, to provide that life-saving assistance so you don’t have to wait for something to come in from outside or make something work.”

“...
The really impressive capability that DOD provided to Sandy support was frankly our ability to let contracts faster than anyone else in the federal government. We didn’t own any of the generators that were brought in. We owned the capability to do contracting immediately.
“We’re called NEMA,” Joseph Shapiro explained, “which is the National Emergency Agency, and we belong to the Ministry of Defense.”

Focusing his remarks on EMP, and NEMA’s process of building an associated official threat document, Mr. Shapiro put this process in a wider threat context. “Israel has many possible threats to our homeland. The Home Front was hurt very badly in the Second Lebanese War, much worse than the actual front, if anyone knows that war. And one of the first decisions after the war was to create NEMA.”

The actual process he said, can be somewhat complex. Threats are “owned” or allocated to different agencies or ministries. “Probably the EMP threat will be somewhere in the energy department with Dr. Shlomo Wald that will be actually responsible for the threat.”

What is NEMA’s role? “We build a comprehensive threat analysis document, and the idea is to present the decision makers in a focused and orderly manner what the primary threats are on the homeland. And where to recommend the priorities for those threats.”

The document, he explained, is actually based on a threat scenario, designed as the “probable worst case.” What is the impact of these threat scenarios?

“And to that scenario, we expect our different agencies to prepare. It’s a management decision.”

This process includes a prioritization recommendation, based on several different metrics. “One is its likelihood, one is its severity and one the economic [impact].” However, this breakdown can be misleading. “When we talk about likelihood, likelihood is not always a statistic. It could also be an expert’s way of looking at things.”

Joseph Shapiro, Director of Threat Scenarios Department, Ministry of Home Front Defense, Israel

“...We build a comprehensive threat analysis document, and the idea is to present the decision makers with the primary threats on the homeland, and recommended priorities for those threats.

When we talk about likelihood, it is not always a statistic. It could also be an expert’s way of looking at things.”
He used NEMA’s work on EMP to illustrate this process.

“Let’s take EMP as an example [of likelihood. It’s hard to say … what kind of cycle [would be relevant] … It could happen any time. So it’s not just a statistical [analysis], it’s an expert’s way of looking at things … And when we speak about likelihood, we also look at assessment and motivation to execute the threat against us.”

What other factors does NEMA take into account? Severity – Casualties, economic effects, impact on national morale and impact on “life routine” or the national agenda. “And economics is not only the cost of the answer itself, but mostly the cost of not preparing an answer. That could be a major factor.”

Duration is also an important consideration. How long does it take to recover?

In summary, he said, the conclusions of their analysis for the EMP threat place it “high” for each of these factors. “Which will bring us to have to include it inside our [official threat] document.” And Israel, he suggested, “could also be a test case [for similar analyses in other nations]. “Because it’s very easy by us to do this work because we only have one electric company …, and also all the agencies … they’re all at the [national] government level, not at the local level.”

What comes next? “We have to go to see what it actually does to the different agencies, health, communications, finance, security and defense, transportation, [and the ] food industry.” And, he continued, water. “Almost the entire water system [is dependent on] electricity.”

“I imagine that within the next year we’ll probably incorporate [these added sectors] inside our comprehensive document.”
Panel 4 | Non-Government Organizations - Emergency Community Support

Eddie Blackmon, Meir Elron and Avi Schnurr spoke of the roles of the NGO sector in planning for black sky events. These roles span two different categories, corresponding to the two relevant classes of NGOs – those involved in education and research, and those focusing on mass care.

Speaking from the perspectives of educational and research NGOs, a fundamental theme was the need for significant, incremental improvements in advance planning to prepare for severe, long duration power outages, including both resilience investment and developing well-coordinated, whole community response. The EPRO Handbook project, and a companion Executive Steering Committee are designed to help facilitate such planning, especially in helping build connectivity with the many public and private sectors that have a role in whole community response.

Ultimately, such preparation must include planning for public education and communication, both to prepare people for severe outages, and for communication during recovery.

Mass care NGOs have unique and critical roles in disaster recovery, and their support will be particularly vital in both supporting restoration and in saving and sustaining lives during recovery from black sky hazards. From mass care feeding to focused support for power restoration teams and their families, and first responders, NGOs have trained, credentialed volunteer teams, including experts with experience in the power industry, law enforcement and other professions relevant to recovery from major outages.
BGen Meir Elron opened his remarks by commenting that security issues have been and remain paramount in Israel. “Presently we are in a situation … that we are really threatened constantly. While we talk here in London, in the last few days, dozens of rockets have been launched against our civilian towns in the southern part of Israel. According to the official scenario, … we might have to face a scenario in which we are attacked by more than 1,000 rockets and missiles a day for a period of more than 30 days.”

This, he suggested, could be an important metaphor for a more general phenomenon. Threats, in general, he pointed out, are constantly growing. “And the question is to what extent our response capacity is keeping up with the increase of a threat.”

General Elron focused on two different, basic elements critical to addressing national scale crises. The first of these elements addressed the need for well coordinated government response.

“I’m quite concerned about the possibility that actually we are talking about a situation in which the gap between the threats and the responses are actually widening. And this is mostly not because of the threat itself, but more so because of our own capacity to deal with the threats properly.”

The focus of his concern, he went on, is on the ability of modern governments to build responsive, well-coordinated teams that can manage national scale crises. “It’s a universal thing. How we connect in the best way in times of crisis, how do we connect the government or the governmental agencies, or the different upper systems with society, with people at large?”

“Once we understand that we cannot totally prevent major disruptions, we have to shift the priority to put more resources into resilience.”
The second element is resilience. “[Once] we understand … that we cannot totally prevent the major disruptions, and we know that there is no hermetic solution or response to these issues … we have to shift the priority and to put more emphasis and more resources on the issues of resilience.” What is resilience? “To me, it means to facilitate the options of a quick recovery … of the system.”

Finally, he said, “We have to think in advance how we activate and how we exploit, so to speak, the population itself and the community itself, in order to enhance the resiliency of the system in times of crisis.”

The population in a major crisis can be vulnerable, and if resilience planning does not go far enough, lack of preparation and information can greatly amplify this vulnerability. On the other hand, a properly prepared population can be an important asset.

“If possibly we are talking about the public at large, in terms of resiliency, we’re talking about its capacity [not to bounce back] but to bounce forward, to an enhanced position. So that next time disruption hits us, the population at large … will be more resilient and more ready.”
Eddie Blackmon began by recalling where he was a week ago. “I was in Pelger, Nebraska, after two tornados went through this small town of 350 people. I’m standing in the road with the sheriff … He’s there directing traffic. And I walk up and I say, ‘Sheriff, do you not have anybody else that can direct traffic?’ He said, ‘No, I need this. I need to see my people. I need to see how they’re doing.’"

The realities of the small town of Pelger, Nebraska may have important lessons for far larger disasters. “That day I’m there,” Mr. Blackmon said, “1,800 spontaneous, unsolicited volunteers show up in a town of 350. Overwhelming the emergency management system that was set up. They turned to us and said, ‘Can you manage these volunteers?’ and we said we’d do our best.”

It is crucial to understand, Eddie Blackmon explained, that to be effective, volunteers need to be selected, trained and properly connected to resources and needs. Spontaneous untrained volunteers, rather than being helpful, can become a serious problem. “There are two types of volunteer groups out there. One is the unsolicited volunteers. They’re going to come. And whatever this event may be if they can show up, they will. And there’s going to have to be a system for managing them, either through government or through non-government organizations.”

“The second group is your group of volunteer organizations that are active in disasters. Number one organization we think of when we talk about it is American Red Cross, Salvation Army, Southern Baptist Disaster Relief, Samaritan’s Purse. A new volunteer group on the scene that’s doing a great job on recovery and cleanup is Team Rubicon, former military guys that are coming in.”

These volunteers, he said, bring with them skill sets, training and local situation awareness that are critical in handling disasters. “You don’t understand the issues of transportation. Well, we do. Many of our volunteers have been in very difficult situations, even

“Unsolicited volunteers are going to come, and there’s going to have to be a system for managing them.”

“I’m standing in the road after the tornado with the sheriff … He’s there directing traffic. ‘I need this,’ he told me. ‘I need to see my people. I need to see how they’re doing.’”
in the military.” In Haiti and elsewhere, he said, “we learned to be resilient. We learned to be flexible.”

What does this mean for helping with power restoration? “Now, with the power companies, what are ways that we can assist? I think number one is in mass care feeding. Other areas of capability, one thing we like to do as Southern Baptists is we look at the [personal needs of the] first responders. Whether it be your guys on the line with the power companies, or your local law enforcement, we ask what are your needs. Does work need to be done at your home? Does your family need childcare? Does your spouse need to be able to get out and take care of things because your home’s been affected?”

More generally, he went on to mention a variety of other needs NGOs can serve. Debris removal, he said, is huge. “In Hillsboro County in Florida, sheriff’s department has an agreement with our disaster volunteers, that they will ride with the deputies right after a hurricane or an event, and will help clear the roads. We’ll put our chainsaw teams with the deputies, and if roads need clearing, we can do that.”

And NGO volunteers include highly trained technical experts. “Many of our volunteers, in all these organizations across the country, are a lot of your guys who have retired out of the power companies. … We have retired law enforcement, we have retired military.” And in addition, he said, people with specialized knowledge will frequently become the trainers for volunteer teams to deal with different disaster scenarios.

“Our volunteers are trained, we’re credentialed according to FEMA’s regulations,” he said. “There’s a partnership here that’s available, that we can assist in these situations.”
Avi Schnurr, CEO and president, EIS Council

“There are excellent reasons to be optimistic,” Avi Schnurr began. “And what I’m seeing is on the part of government, on the part of industry, on the part of NGOs, in the United States, the United Kingdom, Israel, Finland, Norway, a number of other countries that are not here, there is an excellent start at dealing with black-sky hazards.”

To a large extent, he said, this can be characterized as a starting point. Much remains to be done, and one vital aspect of this work is building effective partnerships with NGOs, in two categories.

The first of these categories is mass care NGOs, and their role in Emergency Response. “These NGOs represent a very important dimension in the United States, relating directly to a capability embedded in law. If there is a new dimension, perhaps it is connectivity with the power industry.”

The other aspect, the other category is NGOs involved in education and research. “The job of NGOs in the education domain really is, I think, the kind of thing that we’re doing here. Bringing people, bringing organizations together to help make progress at putting pieces together that otherwise would remain separate.”

This educational mission, he said, is central to the work of EIS Council, and the origin of the EPRO Handbook project, and the companion EPRO Executive Steering Committee. Based on the two days of the summit, he offered a few perspectives on next steps for those projects.

“On black-sky hazards, there are two varieties of things I think that are missing,” he said. First, “I’ve heard a number of people say we need more help understanding what are mitigating options for emerging threats.” Electromagnetic threats – EMP and severe space weather – are good examples, as the newest set of emerging black sky threats.

“And the other aspect is interconnectedness.” As some of speakers mentioned, there are good reasons for some of the limitations on connectivity of government agencies, sometimes referred
to as “cylinders of excellence.” “Nevertheless, there are important reasons that these stovepipes, if you will, need to be connected. One of the functions of educational NGOs is to provide that kind of connectivity.”

On the EPRO Handbook, he offered several thoughts. “I think it’s important that it be understood this doesn’t address by any means all the different kind of hazards that are relevant here. It is intended to address black-sky hazards, in support of the relevant organizations that are doing the real heavy lifting, the real work. Meaning the power companies, meaning the Department of Homeland Security, FEMA, the Department of Energy, and the emergency support NGOs.”

However, he said, the evolving Handbook process can help with informal planning and connectivity, to help amplify the work done by these organizations, and help support the whole community planning that will be critical to recovery from severe outages.

“This kind of process is really only useful if it’s not words, if it actually gets started,” he said. “I would like to announce that our intent is to have the first meeting of a focused EPRO Executive Steering Committee in November. Terry Boston … has volunteered to be the chairman for this steering committee.”

Mr. Schnurr went on to talk about “a few dimensions that we haven’t really been talking about, that you won’t find in the current edition that Paul put together with a lot of help from everyone here, and others.” The international dimension, he said, is critical, but not addressed in the Handbook. Why is it important? “We all live in a global marketplace. And if ideas are not present in the marketplace, they don’t really last.”

And there is much that nations can learn from each other. Norway and Finland, he pointed out, have done very advanced work. “New Zealand has some excellent information that they would like to bring to this community. Israel is also becoming a leader in grid protection against electromagnetic threats.

“**It is important that it be understood the EPRO Handbook doesn’t address by any means all the different hazards. It is intended to address black-sky hazards, in support of the relevant organizations that are doing the real heavy lifting.**"
Mr. Schnurr concluded his remarks with a look to the future. The important question, he suggested, is: “How much needs to be done and when does it need to be done?”

In other words, as we look at black sky hazards, “What is the absolute minimum for these various threats that we need to get started, so at least we’ll have a recoverable situation? And then over time we can talk about how you add incrementally to that minimum.”

In that regard, he said, there is a well-known saying: “Better is the enemy of good enough.” And I think in this dimension it’s exactly correct. If we imagine that we must do the very best that we possibly can and completely resolve any of these black-sky hazards, we’ll never even get started. We have to look for what is the minimum increment, aim at that as the starting point.”

**The important question:** What is the absolute minimum for these various threats that we need to get started, so at least we’ll have a recoverable situation? And then over time we can talk about how you add incrementally to that minimum.
Conclusions
Where Do We Go From Here?
In the final panel, James Arbuthnot, Terry Boston, Bill Bryan, Joe McClelland and Dr. Shlomo Wald came together to conclude the summit, focusing on the question, “Where do we go from here?” They highlighted many of the themes mentioned frequently during the two-day event, especially the need for concrete action plans that address both pre-event resilience investment, and whole-community response planning. As many speakers mentioned earlier, such planning must provide for effective, widely coordinated leadership during the recovery process.

Regulatory measures were mentioned as an important element of resilience to black sky hazards, but the panelists did not see regulation as a “silver bullet.” Regulation typically creates a foundation for further action, and must be supplemented by best practices implemented in a tiered, prioritized fashion based on critical need.

It was broadly acknowledged that the power grid and other lifeline utilities are now regularly subject to attack, with malicious players preparing to expand beyond today’s cyber and physical threats to IEMI and EMP. Both of these electromagnetic hazards were highlighted as important emerging threats, now acknowledged by power companies, that will require incremental investment.

Tools for restoration and response were also mentioned, including emergency communication, provisions for the fuel and backup generator replacements and support for restoration crews, all of which will be essential to bridge the period during restoration from black sky hazards. In some cases, research and development can be important to develop tooling that can speed restoration from such events.
Where do we go from here? Reviewing next steps for several black sky hazards, James Arbuthnot began with electromagnetic threats, where progress has been slow, he said, since “governments are all bad at providing for high-impact, low-probability events.” In that regard, Mr. Arbuthnot reiterated a point made by a number of speakers, that assigning a probability level to such events is not helpful or valid.

On other hazards, “namely cyber and catastrophic natural disasters … since similar approaches are needed to both of those two categories of threats, we’re gradually able to put in place some answers to these problems.”

Overall, he said, the key must be to convince decision makers that black sky hazards must be addressed. “Once we’ve begun to persuade our leaders that these things are going to happen, then we can begin to build the solutions. And here I believe we have to do that incrementally.”

If we can continue to make progress with leadership, we can begin taking concrete measures to address severe hazards. “We need to analyze all of the things that go into overall resilience, building maintenance schedules that are effective, building proper training that is effective. Dealing with inventories so that we have a sufficient degree of spares. All of this has to be done.”

“But more than anything else in my view, we need to educate and communicate with the public.”

“My final thought is this. I think that the word of the conference has been incremental. I’m impatient. I want to see solutions to all of this not tomorrow but today. But if incremental is what I’m offered, it’s significantly better than: ‘Oh, for God’s sake, go away.’

“We need to analyze all of the things that go into overall resilience, building maintenance schedules that are effective, building proper training that is effective. Dealing with inventories so that we have a sufficient degree of spares. All of this has to be done.”

I’m impatient. I want to see solutions to all of this not tomorrow but today. But if incremental is what I’m offered, it’s significantly better than: ‘Oh, for God’s sake, go away.’
“Where do we go from here? The question is how far do we go?,” said Terry Boston. “Industry is willing to take prudent steps to protect against GIC and EMP.” However, “knowledge about the most effective shielding and protection of equipment is often protected by the classified curtain.”

One of the most important reasons to take such steps, he said, is for the deterrent effect. “We don’t want to create a situation where we create motivation for people. I agree with John, the best deterrent that you have is to have things protected. Doing nothing is not an alternative, but regulatory cost recovery has got to be resolved.”

Terry Boston felt GridEx II was an important step. “Gerry did a great job,” he said. “35 million people [affected in the exercise]. This could be much bigger than that. GIC, EMP I think you start with the black-start cranking paths. You take this one small step at a time, but you’ve got to get started … we’ve got to start an action plan.”

Referring back to an earlier comment by Thomas MacLellan, “Fukushima was not caused by an earthquake or a tsunami. It was caused by the loss of offsite power to a nuclear plant. If you think about that for just a minute, it changes your emergency preparedness mentality.”

Resolving this does not mean looking for a silver bullet. “What we need here is silver buckshot, lots of little things that we can do, to improve the risk that we have … We must define [those] that we’re willing to do, and then we must do so. “

Terry Boston concluded by highlighting several examples of cross-sector resilience and response planning that were raised during the summit.
“Fuel for emergency generators, we talked a bit about line trucks, Red Cross, Baptist feeding facilities. You can’t cook food without the emergency response. We need to solve some of these simple problems. Sandy, crews came with cooking facilities. They came out of the hurricane zone. They had experience.”

Hurricanes, in fact, have been the source of many lessons learned. “We have learned a lot from these hurricane experiences. They are the largest thing that we’ve seen that would be even close to the EMP, but Sandy had 8.5 million meters … some 18% of the population on that.”

Concluding, he said, “We must lower the risk for cyber attacks, kinetic attacks, GIC and EMP. We need to plan to have a system that can take a licking and keep on ticking.”
Based on the summit presentations, Dr. Shlomo Wald prepared six points that he felt should be highlighted.

1. **RECOGNIZING A NEW EMERGING THREAT - EMP:** “First of all, we have to be prepared against an EMP event, the most serious EMP event, let us say malicious nuclear attacks.”

2. **BUILDING A CREDIBLE, ACTION ORIENTED PLAN:** “EMP should be considered [an official] reference threat. That means you have some plan in your drawer, [with actions taken in advance] in order to mitigate the event.” Why should EMP be placed on this list? “It is not a simple scale-up of existing solutions [for less severe hazards],” he said. “It covers a very large area … and has a simultaneous, multisystem effect … with cascading impacts on many other systems.” An event of this magnitude could also “initiate opportunistic acts of criminals, terrorists, or even neighboring [enemy] countries. EMP will be a gate opener …”

Dr. Wald included in his remarks a short list of critical priorities for mitigation of this unique electromagnetic hazard. “We need a safe way to share information,” he said. “And [for rapid restoration] we need an automated way to identify system faults.” Given the scale of the event, while only a fraction of computers and low voltage electronics will be affected, with system controllers down, finding those problems could be logistically complex and time consuming.

3. **International standards for civilian infrastructure protection against EMP:** Not military standards, he said. “Civilian standards, [which] are different from military standards. And international, because I think that international collaboration is essential.” The International Energy Agency (IEA), he suggested, might be an appropriate vehicle for such standards, and could potentially also act to broker international mutual assistance, including maintaining inventories and sharing of critical, long lead hardware in the aftermath of EMP or other black sky hazards.
4. **Assured, whole-of-nation response:** “You have to have command and control that consolidates all the stakeholders together, to decide priority in real time.” Loss of the chain of command is a serious concern for any black sky hazard, he said, and this includes planning for broadly available, survivable emergency communication. And given the complexities and competing priorities in recovery from an EMP or other black sky hazard, provisions must be made for broadly coordinated recovery process that includes all government, corporate and NGO stakeholders.

5. **Research and Development:** “There is a lot to be done in order to have all the technology capabilities to mitigate EMP in the civilian market, including hardware and software.” For hardware development, an example would be the fault identification system he mentioned previously, or an emergency communication system. “Then for software, we have to do detailed operational research of all critical elements, in order to define priority and to define the interconnection between critical elements.

6. **Public awareness:** This is extremely important, he said. “If people are aware of this situation, they can respond in a much more reasonable way.”
Bill Bryan echoed a common theme in his summary comments. “We need to be better prepared, and to have better planning,” he said, before we can face black sky hazards. And in regard to those hazards, “We need to better scope these threats.”

He also highlighted the importance of training and exercises. “Lessons learned are not learned unless they’re applied,” he said. And there is considerable staff turnover in both corporations and government. All of that makes exercises particularly important. “And we learn a lot from all these exercises.” But not, he warned, without a foundation of better preparation and planning. “We need to follow through on some of the recommendations.”

In particular, he highlighted an issue that must be faced for any national scale event. “The governors manage these response activities. However, when you start crossing into different states, there can be problems … There are different policies and procedures and processes in laws and regulations [for different states].” That, he said, became an important limitation in Sandy.

He concluded with a comment that was a frequent theme of the summit: the need for whole-of-nation response and coordination. “You need to start inviting all the stakeholders to the table.”

“"When you start crossing into different states, there can be problems, with different policies and procedures and processes."

“"Lessons learned are not learned unless they’re applied. And we learn a lot from all these exercises."
The final speaker at the summit, Joe McClelland, concluded the session on a sobering note, highlighting three categories of black sky hazards: cybersecurity, physical attack and EMP/IEMI.

**Cybersecurity**

Speaking to “anyone … that owns or operates utility systems – your systems are being actively targeted and they’re under attack.”

“I want to make that very plain. I want to tell you that in the open, and be as direct as I can. Before I came to the platform,” he said, “one of the things that I did in advance was I googled the phrase "energy infrastructure targeted for attack" and I literally came up with … hundreds if not thousands of websites not only describing the attacks, but advocating attacks, and encouraging attacks on infrastructure.”

As another example, focused on current cybersecurity news, “a news article just came out today. … Dragonfly, according to Symantec … is a variant of Stuxnet. It’s specifically targeting European and US control system networks, the networks that enable the operation and control of the power grid. It’s purportedly written by the Russians, and it’s extremely sophisticated. It’s positioned itself in the networks.”

This, Joe McClelland pointed out, is not an abstract issue, but an urgent and immediate problem. Based on these news reports, “the moment that there’s a conflict, the moment that they feel there’s a good opportunity that benefits them, they can start to operate your control systems,” he said.

**Physical security**

He also highlighted expanding concerns for physical security. “In Yemen, for the first time a nation’s [power grid] has been brought down by a physical security strike. Gerry Cauley,” he said,
“provided some details about the Metcalf attack.”

In other words, the total dependence of modern societies on their critical utility infrastructures is now broadly understand, along with the vulnerabilities that implies.

“Fortunately,” he said, “there are best practices.”

**EMP and IEMI**

He concluded his remarks by turning to electromagnetic threats. “On EMP and IEMI, I guess the first question I would have for the crowd is, ‘Do we believe it? Is this a viable attack vector? Is this real?’”

“I’d like to talk to anyone that doesn’t think that it is,” he said. “There are organizations now that are selling the equipment. There are online courses. These are lethal devices. They’re being perpetrated, they’re being planned and built and disseminated for the sole purpose of attacking control systems.”

For all of these concerns, he said, in the U.S., there are resources. “There’s the Department of Energy, there’s the Department of Homeland Security, and there’s the Federal Regulatory Energy Commission. We’ve got dedicated resources set aside to bring best practices to whoever asks for it.”

He also spoke about the difference between regulatory standards and voluntary best practices. “The standards are not meant to be best practices. They’re meant to be foundational practices. Think of the pyramid, they span across the foundation. They are not adequate,” he said. “They are not adequate for the most critical facilities and they’re not adequate against nation-state threats.”

But best practices imply additional cost and effort, making tiered planning important to implementation. “The next question is where do we implement these best practices? We had lots of discussion about tiering. Everyone accepts the approach. So what are the tiered assets?”

“The thought isn’t to make these facilities impenetrable, but to introduce uncertainty,” he said. “If we introduce uncertainty, we’ll drive the adversary off the targets.”

**What are the impediments?**

“I heard David Owens talk earlier about potential impediments. Logistics, for the housing, for the utility crews that will be tasked to come in and restore service.”

“Are EMP and IEMI real threats? There are organizations now that are selling the equipment. There are online courses. These are lethal devices being planned and built and disseminated for the sole purpose of attacking control systems.”

Regulatory standards are not meant to be best practices. They are meant to be foundational practices. They are not adequate for the most critical facilities and they’re not adequate against nation-state threats.

The thought isn’t to make these facilities impenetrable, but to introduce uncertainty. If we introduce uncertainty, we’ll drive the adversary off the targets.”
“I’ve heard Avi Schnurr say in previous conferences that we’ve had two types of societies, there’ll be the societies that prepare and continue, and there’ll be the societies that are no more. If it’s an effective EMP attack, it will be on that scale.”

As for other hazards, the key, once again, is tiering. “The most critical facilities should be identified. They should be tiered off, and best practices should be encouraged at those facilities. How do we encourage those? Who are the decision makers? How do we bring the decision makers to the table? How do we get them engaged with the issue?”

In answer, he referred to something he noticed at the summit dinner, which took place in the former underground bunker known as “The Churchill War Rooms. “I was at the underground bunker and I saw a conference table that Prime Minister Churchill was using during the conflict. I also was at Parliament, and took a tour, and saw the House of Commons side and then the House of Lords side.”

“I saw marks on the tables that Churchill used. Where he could pound his cygnet ring to drive his point home, if progress wasn’t being made, he’d pound the cygnet ring. And I guess the challenge to this group is if he walked through that door today and he saw the progress we were making, could we prevent him from pounding the conference table and marking the EIS structure itself?”

“The most critical facilities should be identified. They should be tiered off, and best practices should be encouraged at those facilities.”
Summit Reception

The EISS V reception took place in the Churchill War Rooms, the secret underground headquarters that were the nerve centre of Britain’s war effort in World War II.