Summit Report

EISS VI | WASHINGTON 2015
Electric Infrastructure Security Summit
Whole Community Collaboration

THE SIXTH ANNUAL WORLD SUMMIT ON INFRASTRUCTURE SECURITY
The sixth 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. With its theme of “whole community collaboration,” EISS VI focuses on a unique requirement for recovery from EMP and other Black Sky hazards: Planning, training and ongoing coordination among the full set of lifeline infrastructure owners and operators, and their government, corporate and NGO partners.
Electric Infrastructure Security Summit VI
Summit Report

Published:
July 18, 2016

Principal Editors:
Yedidya Sinclair
Avi Schnurr

Contributing Editors:
Sarah Schnurr
Dr. Chris Beck

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

"Whole Community Collaboration"

There is broad agreement on the importance of resilience investment and restoration planning. Collaborative planning by and in support of our interdependent, critical utilities is essential to strengthening the resilience of lifeline infrastructure against “Black Sky” hazards: Unusually severe malicious and natural threats that risk long duration, multi-region outages to assure grid continuity regarding “black sky days”: extraordinary and hazardous catastrophes utterly unlike the blue sky days during which utilities optimally operate.

EISS VI focused on this objective. Summit sessions reviewed the current state of utility, government and NGO planning to address such hazards, and examined next steps required to address the unique coordination challenge they represent.

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.

EIS Summit VI Dedication

EISS VI, in 2015, was dedicated to the memory of Dr. Jack Templeton, a doctor, philanthropist and leader with unflagging enthusiasm to leave the world a better place than he found it. He succeeded.
Executive Summary
Executive Summary

EIS Summit VI took place at the U.S. Capitol Building, Washington DC, in July 2015. This was the largest summit held so far in the EISS series, bringing together senior leadership from government, the private sector, utilities, academia and NGOs representing eighteen countries to discuss protection against critical threats to lifeline infrastructure.

The theme of EISS VI was “Whole Community Collaboration,” with a focus on collaborative planning to support critical utilities. Strengthening resilience of lifeline infrastructure against electromagnetic threats and other Black Sky hazards, speakers emphasized, must go hand in hand with recovery – preplanned preparations to save and sustain lives in such scenarios.

Collaboration, across public and private, government, NGO and utility sectors was broadly identified as key to these twin objectives, tying in well with the summit theme. Power outages causing cascading failures in other utilities and services were highlighted as the central concern, with impacts to transport and distribution of food, fuel and other resources. Speaking of different dimensions of the public-private partnership, speakers concurred on a fundamental conclusion: Planning to protect and mitigate against such an event is essential, and must involve coordination and cooperation among all involved sectors.

A number of areas received particular attention by speakers and delegates:

1. **The Importance of cross-sector planning, with overall recovery coordination.**

Sector interdependencies make cross-sector planning crucial. As Jonathan Monken from EIS Council told the delegates, “A catastrophic power outage is a whole community event. Nothing can be handled in isolation.” For example, in restoring the electric grid, relationships with the transportation sector will be vital. Transporting large, Extra High Voltage (EHV) transformers will require detailed prior planning. Likewise, ensuring that emergency generators – of adequate sizes and numbers -- can be moved to where needed is another important challenge, as is the need to plan for production and distribution of emergency fuel in such scenarios.

James Fama from Edison Electric Institute pointed out how the value of cooperation proved itself recently after the attack on the Metcalf substation in San Jose: “The STEP folks … put a call together. They had the relationships in place. They all knew each other and within hours they had basically identified … who had what Pacific Gas & Electric needed for that substation… That’s the power of relationships.”

Other speakers explored specific ways in which government agencies can support lifeline utilities. While emergency generators and fuel were highlighted by many, a number of other areas were also identified, including emergency communications, cross-sector coordination, regulatory sector engagement, and wide information sharing and decision-support are just a few examples of the wide-ranging discussions.

Given this wide range of support requirements, as Paul Stockton, former US Assistant Secretary of Defense put it, we will need tools to help decide “who gets what in such a way that we will save and sustain the most lives, and really facilitate the restoration of crucial infrastructure.”
2. Electricity is key to everything

Speakers reiterated how intensely dependent our technologically sophisticated economy and infrastructure is on electric power. As US Congresswoman Yvette Clark put it, “without electricity, banks close down, food goes bad, sewage and water plants don’t function and human life is threatened.” Rapid power restoration is thus of paramount importance.

Addressing these issues requires particularly close cooperation, coordination and information sharing between power companies, emergency managers and other stakeholders, a need that was highlighted by joint participation on a single, integrated panel by senior speakers from Wisconsin representing the State’s Public Service Commission, Emergency Management Agency, National Guard and ATC, the State’s primary electricity provider. Panelists focused their comments on the importance of careful cross-communication, between utilities and government agencies, of the kinds of policy and support needed to address Black Sky and other severe hazards.

3. More attention should be paid to water and wastewater as a primary, critical need for saving and sustaining lives

In a Black Sky event, with a catastrophic power outage, the very first, most imminent threat to public health and safety is likely to come from the cascading effects of the loss of electric power on the water and wastewater sector. Speakers pointed out that water has not always received the attention it deserves as part of critical lifeline infrastructure; people are so used to turning on a tap and receiving clean, safe water, 24/7 that, ironically, inadequate attention has been paid to the urgency of critically needed water and wastewater infrastructure upgrades and expanded resilience investment.

Dr. Paul Stockton, joined in his comments by Dr. Sally Leivesley, argued that among the chief goals in protecting our cities should be avoiding the need for emergency, unplanned mass evacuations, with protection of water and wastewater assets representing the primary need to avoid this tipping point.

Speakers also pointed out the numerous interdependencies between the water and power sectors; pumping water requires power, but many power plants also have significant requirements for pumped-in water. Cross sector collaboration, for these and other sectors, and including State and Federal Regulators will, therefore, be an important part of the process.

The regulatory sector, in fact, was identified by many as playing an essential role in setting affordable standards of protection and resilience for utilities – and helping to define “affordable.” Speaking on this point, Chris Train from National Grid U.K. pointed out that risk mitigation and resilience-focused regulatory policy needs to be balanced with market incentives to ensure that infrastructure operators take necessary protective action, in realistic market environments.

4. A wide set of emerging Black Sky hazards are receiving growing attention

The potential impacts of a severe space weather event on our critical infrastructure have captured the attention of senior leaders in the White House, in Congress, in Federal and State
agencies, internationally, and across the private sector. The Summit heard from the White House Space Weather Operations, Research and Mitigation (SWORM) Task Force, and from commissioners, CEOs and senior executives of FERC, NERC, NOAA and other organizations about steps they are now taking.

Malicious threats also received significant attention. DoD Deputy Assistant Secretary Charles (Chuck) Kosak told delegates, “Today’s asymmetric threat environment is unprecedented. And it’s worsening,” he said. “We have adversaries, nation states, as well as transnational terrorist organizations that... are continuing to increase the frequency of attacks here in the homeland, and their sophistication is increasing as well.”

Successive speakers identified EMP as an increasingly well-established element of offensive and defensive military planning today, by both state and non-state actors. Congressman Trent Franks quoted from an Iranian military document referencing EMP as a weapon to damage or disable power grids. Speakers also emphasized cyber-threats as a rapidly growing threat vector for critical national infrastructure. Speaking of the U.K., Lord James Arbuthnot declared, “Our national grid is coming under cyber-attack every minute of every day... I want to hear no more of this phrase “low probability, high impact.” The impact is potentially devastating... But the probability is not low. In fact it’s not even probability. It’s constant, provable fact.”

In the context of the summit theme, cross-sector collaboration was broadly identified as a critical need to ensure that adequate, preplanned resilience investment and recovery planning is put in place to allow for effective recovery from this full set of severe hazards.

5. Exercises are critical for addressing hazards of this magnitude and, increasingly, must be hosted as cross-sector efforts.

The summit was preceded by EPRO ESC Summer, 2015, framed by a Black Sky Exercise exploring options for recovery from a long duration, multi-region outage. For this exercise, the threat identified was an EMP attack, with two modules addressing an event today and in five years, after assumed far greater preparedness. Terry Boston, PJM CEO and Chair of the EPRO Executive Steering Committee, summarized the results: “Needless to say,” he pointed out, “we have much better response to this drill after preparing for five years.”

6. International cooperation is an important dimension of cross-sector coordination

Speakers also paid tribute to the important role of international coordination and knowledge-sharing, highlighting particularly the work of EIS Council in helping the U.S. work with allied nations to mutually benefit from such sharing, becoming more aware of infrastructure threats and enhancing preparations that address them.

In this vein, Dr. Sally Leivesley spoke from a U.K. perspective of the potential to work internationally to restrict attack vector options for cyber threats. Koby Wimisberg from Israel urged the summit, “We need to be a community and we need to share with each other, and as such, I believe that every move towards strengthening the community strengthens all of us.”
Session One

“Where are we?”

Lifeline Infrastructure Resilience Today
The White House Space Weather Operations, Research and Mitigation Taskforce


The opening panel surveyed the work of the Federal Space Weather Operations, Research and Mitigation Task Force, (SWORM) which brings together multiple US government departments and agencies. The establishment of the Task Force reflects a recognition at the highest levels of government that severe solar weather, together with other potentially catastrophic threats to electrical infrastructure, could have devastating impact on U.S. and other developed world economies and societies. The seriousness of this hazard is acknowledged internationally and has been discussed between the US President and the British Prime Minister.

Speakers stressed the acute electricity dependency of all of our technology-based infrastructure sectors, including water, communications, transportation, health services and food systems, all of which are critical for our prosperity and security. Given the interdependency of these sectors, a whole community approach to resilience and recovery planning is essential. All stakeholders, including federal, state and local government, lifeline utilities, critical private sector infrastructure and NGOs need to work together to develop and implement protection plans.

In their remarks, the panelists made it clear that the key, now, is not merely to develop a protection strategy, but to work urgently on its implementation.
Introducing the work of the Space Weather Operations, Research and Mitigation (SWORM) Taskforce, Dr. Baker reviewed the primary concern – the potential for serious power grid disruption on national scales, associated with damage that could lead to continental scale outages, potentially for weeks or months.

“Impacts on the power grid would quickly spread to be of continental scale. Under the worst scenarios, policymakers, emergency preparedness workers, and health practitioners could be left powerless and out of touch through much of the societal infrastructure for extended periods of time.

Dr. Baker highlighted a recent, extreme solar event as an example, a “near miss” that, had it occurred one week earlier, would have hit the earth. “A direct hit by an extreme coronal mass ejection, as they are known, such as the one that narrowly missed earth in July 2012, could cause widespread power blackouts,” he said.

Dr. Baker called for increased effort, nationally and internationally, to prepare for such an event. “It is crucial that policymakers on the national and, indeed, on the international level develop effective operational space weather systems and prepare appropriately to mitigate and, ultimately, to recover from the effects of severe space weather events,” he said.

Summarizing, Dr. Baker said that we have now become aware that such extreme solar events happen on a regular basis. Will a “debilitating, severe space weather event” strike the earth? “Most people involved in the study of solar storms realize that it’s not a question of if,” he pointed out, “but when.”

“This is crucial that policymakers on the national and, indeed, on the international level develop effective operational space weather systems and prepare appropriately to mitigate and, ultimately, to recover from the effects of severe space weather events. It is not a question of ‘if,’ but ‘when.’”
Tamara Dickinson focused her remarks on the growing awareness and concerns regarding severe space weather, among senior leaders in both government and the private sector. “The potential impacts of a severe space weather event on our critical infrastructure has captured the attention of senior leaders in the White House, in Congress, and across the many departments and agencies, both nationally and internationally, and across the private sector,” she said.

She provided several examples of recent or pending government action. “The NASA Authorization Act of 2010 codifies space weather as a significant threat to the nation,” she explained, assigning responsibility to the White House Office of Science and Technology Policy (OSTP) to address “potentially devastating impacts of space weather events.” In April of 2013, OSTP released a report: “Space Weather Observing Systems: Current Capabilities and Requirements for the Next Decade,” assessing “the nation’s capacity to monitor and observe potentially harmful space weather events.”

Congress is also working on pending legislation, such as the Critical Infrastructure Protection Act, H.R. 1073, which addresses severe space weather along with an additional focus on EMP. The Federal Energy Regulatory Commission has also begun addressing this concern. “FERC recently approved a reliability standard designed to help mitigate the effects of geomagnetic disturbances on the bulk power system,” she pointed out.

Internationally, “NATO and the UN organizations, and many individual companies are taking initiatives to assess and respond to the threat.” In addition, “Space weather has been discussed in meetings between the President of the United States and the UK prime minister,” she said, with UK government representatives coming to the White House for follow-up meetings in early 2015.
Ms. Dickinson echoed Dr. Baker’s comments regarding the primary concern, pointing to the potential for severe impacts on our electricity-dependent infrastructure. “Our technology-based infrastructure requires a robust, energy distribution network,” she said. In fact, the “global nature” of space weather events makes this concern unique. “Few other naturally occurring phenomena have the potential to be so far reaching on its impact to mankind.”

Ms. Dickinson concluded by summarizing the mission of the SWORM task force. “The task force was chartered to develop a space weather strategy that articulates high-level strategic goals for enhancing the nation’s preparedness for space weather events,” she explained, and “also recognizes the importance of engaging and coordinating efforts with the private sector and with academia.”

What are the next steps?

Strategy alone, she said, is not enough, and an action plan is being developed. As an issue with such broad, potential implications, government action, she pointed out, is essential. This will require a common strategy, with actions that will be needed from different government departments and agencies. “We must identify the actions that will be most effective in enabling our government partners and agencies to implement the strategy.”

Finally, Tamara Dickinson expressed high praise for the opportunity provided by EIS Summit VI. “This is an exciting and important event,” she said.

“Given the global nature of severe space weather, few other naturally occurring phenomena have the potential to be so far reaching on its impact to mankind.”
Describing her role on the White House Taskforce, Assistant Secretary Durkovich explained that she brings the focus of the Department of Homeland Security “in understanding the potentially consequential and devastating impacts of space weather within the context of how we look at critical infrastructure, security, and resilience.” As a basis for their strategy, DHS utilizes the National Infrastructure Protection Plan and the National Preparedness System. The key, however, is developing a “whole of community” collaborative strategy, including local, state and international government, and private sector stakeholders.

How is this done? A two-way information sharing process is a key part of this process. In this way, DHS can help “drive capability and capacity, whether it’s training, whether it’s exercises, or whether it’s the development of best practices to mitigate these risks.”

Given the criticality of our infrastructures, and the range of serious threats, this effort is quite important. “Our economic security and prosperity depends on the functioning of critical infrastructure, but so does our national and our homeland security,” she said. “And the range of things that can disrupt them, from cyber criminals and hackers to things like space weather and EMP are increasing as well.” The scope of the hazards that must be addressed is quite broad. “The biggest challenge that we have is that we have to do this in an all-hazards environment. Owners and operators of critical infrastructure face an increasing number of threats and hazards that can disrupt their operations.”

However, addressing the critical issues must begin with a coordinated, collaborative process. How is this done? “This can’t be something that the government does in a vacuum,” she said. “We need to bring the owners and operators of critical infrastructure into the dialog and into the development of this strategy.”

Caitlin A. Durkovich, Assistant Secretary for Infrastructure Protection, DHS

“Our economic security and prosperity depends on the functioning of critical infrastructure. […] And the range of things that can disrupt them, from cyber criminals and hackers to things like space weather and EMP is increasing.”

“…This can’t be something that the government does in a vacuum... We need to bring the owners and operators of critical infrastructure into the dialog and into the development of this strategy.”
Dr. Louis W. Uccellini, Director, National Weather Service, Assistant Administrator, NOAA

Dr. Uccellini explained that the space weather forecasting service, like weather forecasting, in general aims to build a weather ready nation – or, in this case, a “space weather-ready nation.”

“The intrinsic value of a weather forecast,” he noted, “comes from its applications to decision making. And with our mission of protecting lives and property, this connection is very important.” The first step in forecasting is observation. NOAA is improving its space weather observation abilities with a satellite network called Discovr.

The goal of the system is to get better information about solar weather to the decision makers who need to work to mitigate a solar flare event. When a coronal mass ejection occurs, NOAA aims to be able to predict the time when it will strike the Earth and to provide warning alerts to people, especially those involved in operating the electrical grid.

“The research and operational communities have to be responsive to those users of this information that are actually making the critical decisions,” Uccellini stressed. Therefore, NOAA works in partnership with organizations including NASA, DoD, and NSF among others to ensure that the research information they compile is maximally useful to operations personnel and decision makers.

The intrinsic value of a weather forecast comes from its applications to decision making. And with our mission of protecting lives and property, this connection is very important.

The research and operational communities have to be responsive to those users of this information that are actually making the critical decisions,
Rep. Yvette Clarke (D, NY), Chair, Congressional Perspectives
U.S. Congresswoman Yvette Clarke, Co-Chair, Congressional EMP Caucus.

Rep. Clarke underscored the fundamental role the grid plays in our lives and economy. “We simply cannot afford to lose broad sections of the grid for days or weeks,” she warned. “It is our very reliance on the grid that makes it important to anticipate the worst.

Clarke praised the work of the EIS Summit Series in “building an international security framework” to protect critical infrastructure. “This summit series is an attempt to motivate all nations to take the threat seriously and to act,” she declared. “According to studies by congressional commissions and government agencies in the US, UK and elsewhere, national electric grids could be headed for disaster if we don’t change our course.”

Rep. Clarke recalled how, after Superstorm Sandy, she and others learned not to take the electricity grid for granted and to recognize the grid’s vulnerabilities; “Without electricity, banks shut down, food goes bad, sewage and water plants don’t function, gas stations are closed, medicines expire, and human life is threatened…” she warned.

Clarke concluded by committing to continue speaking up to warn people of the serious potential manmade and natural threats to the grid and to exhort them to take the necessary steps to protect against them. She urged all those present at the summit to do likewise.

“This summit series is an attempt to motivate all nations to take the threat seriously and to act.

“Without electricity, banks shut down, food goes bad, sewage and water plants don’t function, gas stations are closed, medicines expire, and human life is threatened…”
Panel 1
Lifeline Infrastructure Resilience to Black Sky Hazards Panel

Panel Chair: Dr. Paul Stockton, Coordinator, EPRO ESC

In this panel, leading representatives of the electrical power and water sectors spoke on protecting and increasing the resilience of lifeline infrastructure.

Among the main areas discussed by the speakers from the power sector were the growing importance of identifying and protecting key cyber assets, the painstaking work being done on procurement, storage and transport of spare transformers, and the vital importance of relationships and cross industry collaboration. The rapid recovery from the recent physical attack on the Metcalf substation in San Jose California was cited as a success story of cooperation.

Speakers noted differences between the U.S., with its decentralized electrical system and the U.K., where the task of protecting electrical infrastructure is generally assigned to the National Grid.

The water industry speakers welcomed the increasing attention to their sector represented by the summit. They delineated the potential public health dangers from cascading effects of prolonged power outages on water and wastewater facilities.

Noting the very low tolerance of consumers for water system outages, panelists discussed how, a whole community approach can increase resilience and lessen the likelihood of community evacuation in Black Sky scenarios. They also emphasized the tight interdependency between the water and power sectors, and the consequent need for joint planning for Black Sky events.
Electric Sector
Gerry Cauley, President and CEO, North American Electric Reliability Corporation

“Lifeline Infrastructure Resilience to Black Sky Hazards”

Gerry Cauley’s presentation focused on NERC’s work to increase the resilience of critical electrical infrastructure against a range of threats. He opened by stressing the importance of preparing for the full set of risks, including both extreme hazards and more conventional, typically weather-related events.

Turning to NERC’s specific activities promoting systems resilience, Cauley first discussed the CIP Version 5 Security Standards due to go into effect in April 2016. He pointed out that these standards marked a shift towards a risk-based control approach to managing the security of the power grid. As he put it, “this shifts the focus….from checking boxes, checking the list to be compliant, to building the best security controls we can have.” Moreover, the new standards are to deal with the whole of the bulk power system, graded according to priority, whereas previously only critical facilities were covered.

As a part of this process of improving resilience, Cauley noted a growing awareness of the importance of cyber assets throughout the system: “All the entities that manage the bulk power system are identifying, and tagging, and inventorying all of their cyber assets, and identifying the priority of those, something that we had not done before. We’re assessing all the vulnerabilities of all those assets.”

Cauley also discussed the new physical security standards about to come into effect. These will enhance resilience by making companies more aware of good practice for physical plant security.

Reviewing recent regulatory standards that address the Geomagnetic Disturbances (GMD) hazard, Gerry Cauley explained that the new standards are divided into two phases.

“\[\text{All the entities that manage the bulk power system are identifying, and tagging, and inventorying all of their cyber assets, and identifying the priority of those, something that we had not done before.}\]
The first part, already in effect, deals with operational awareness and response and includes the analysis and dissemination to power providers of information and alerts regarding solar storms and other severe threats. We see companies going into a conservative posture in regard to those solar storms to ride through them.

The second part of these standards, under development, at the time of the summit, addresses measures to physically harden and protect critical facilities against a one-in-a-hundred years solar storm. Additional beneficial outcomes of the work on GMD standards include the installation of hundreds of ground current measurement devices, thermal monitoring of transformers and the installation of monitoring devices and computer-to-computer communications that enable identification of security threats in real time.

Finally, Cauley pointed to the resilience-building effects of simulation training, including the North American-wide GridEx III exercise. “We have very severe threats simulated on the grid. And we expect that this year’s exercise will be even more severe,” he concluded.
Thomas Galloway, President and CEO, North American Transmission Forum:

Thomas Galloway described how the North American Transmission Forum has placed major emphasis on building resilience over recent years. Comprising eighty member companies, the Forum’s members represent over 85% of the high voltage circuit miles and 85% of the peak load in America. Many of the forum’s program areas are modeled after the Institute of Nuclear Power Operations, created in the commercial nuclear industry after the Three Mile Island accident.

The Forum has focused on developing best practices to foster resilience in transmission systems. “We bring groups of subject matter experts together to talk about the issues, challenges and superior practices in different technical topics,” Galloway explained.

The Forum works closely with the Electric Power Research Institute (EPRI) in this area. Employing an all-hazards approach, they work together on classifying the different types of hazards and developing a structure of superior practices corresponding to the different hazard groups.

Referring to Gerry Cauley’s talk, Galloway remarked that several aspects of the Forum’s resilience planning parallel the work that Cauley described happening at NERC. The Forum is closely following developments in cyber security. It has placed special emphasis lately on CIP-014, the physical security standards. Recent activities in that area have included detailed surveys of members to help identify critical assets covered by that standard and developing reference guides, “to make sure that they’re not only meeting but also exceeding the base requirements of those standards.”

The Transmission Forum also held a very well attended, comprehensive resilience summit towards the end of 2014. The goal of these activities to date has been to disseminate awareness of key resilience concepts and to set the stage for action going forward.
James Fama discussed how his organization’s mutual assistance program has grown and strengthened infrastructure resilience since the acute challenge of Hurricane Sandy. “On the fly” solutions, improvised in the midst of Sandy, have evolved into a systematic playbook.

Fama mentioned a number of EEI’s programs to enhance mutual assistance within the electricity subsector. These include the spare transformer equipment program (STEP), a program that networks companies with spare assets that can be shared (the Spare Connect Program), and a partnership with the North American Transmission Forum to stockpile equipment.

A particular focus of EEI’s work has been developing processes and relationships with key transportation infrastructure providers to enable the replacement of heavy electrical equipment. For example, replacing the large transformers in critical grid substations, were they to be damaged in an EMP attack, would pose complex logistical challenges.

“What if we need to move equipment into those substations? Do we have enough transformers? Do we have the right size transformers, and most importantly, can we move them in an emergency?”

EEI has been working closely with the railroads on solving the transportation issues. This requires addressing numerous mundane-seeming but critical technical details such as ensuring that the railroad has accurate drawings of how a transformer would sit on a railcar, and reliable information on their weight and dimensions.

“...It may sound mundane, but when you get these transportation measures in place, you get the relationships going with the riggers and the rails, you can really shorten your time that it takes to move things in an emergency, because any time we can...take a chunk out of our timeline, that is critical.

“...When you get the relationships going, you can really shorten the time it takes to move things in an emergency.
“It may sound not very glamorous,” Fama acknowledged, “it may sound mundane, but when you get these transportation measures in place, you get the relationships going with the riggers and the rails, you can really shorten your time that it takes to move things in an emergency. Because any time we can…take a chunk out of our timeline, that is critical.”

Fama stressed that relationship-building is an overall priority for EEI, with relationships developed with participants in EISS summits a very positive example of this process. In an emergency, people in the power, transportation or other sectors who know each other could help solve problems faster, even when no official program applies.

Fama used the example of the Metcalf sub-station in San Jose California which was damaged in a physical attack. “Within a few hours all the STEP folks … put a call together. They had the relationships in place. They all knew each other and within hours they had basically identified … who had what Pacific Gas & Electric needed for that substation. There was no specific program for when a substation gets shot up in the middle of the night. That’s the power of relationships.”

“In the case of the Metcalf substation in San Jose California which was damaged in a physical attack, Fama said, The STEP folks … put a call together. They had the relationships in place. They all knew each other and within hours they had basically identified … who had what Pacific Gas & Electric needed for that substation… That’s the power of relationships.”
Dr. Matthew Gardner, Electric transmission Operations Research Project Manager, Dominion.

Matthew Gardner described the three-pronged approach to addressing potential disaster, whether physical, cyber, natural or anthropogenic. The three elements are:

- **Prevention and deterrence**: this comes down to equipment design and hardening;
- **Detection and event mitigation**: the focus here is on instrumentation and data availability;
- **Recovery**: this relies on how we store, stage, manage and protect spares;

Gardner then briefly surveyed Dominion’s preparations to protect against each of the three different components of damage from an Electromagnetic Pulse (EMP) event.

**EMP E3**: To help defend against the EMP E3 pulse effect, Dominion has developed a system of alerts and warnings direct to the appropriate managers and key staff. For the past five years, the company has been modelling its systems to understand how DC currents would flow through the network as a result of the EMP E3 effects of an EMP event.

Dominion has also installed a number of Hall Effect DC current monitors to measure and monitor these effects, and is working with NASA on additional monitoring devices. In the area of equipment enhancement, Dominion is working on better ways to protect capacitor banks and on improvements in the basic design of transformers so they would perform better in an EMP or GMD event.

**EMP E2**: Dominion’s preparations against an EMP E2 pulse from an EMP event are relatively advanced. As Gardner put it, “EMP E2 for us looks a lot like lightning…we are a Mid-Atlantic service territory. We see quite a bit of lightning activity.” Consequently, protecting from lightning and lightning-like damage through installing arrestors and high-frequency grounding is already a part of Dominion’s activities.
EMP E1: As part of its equipment strengthening measures against an EMP E1 pulse, Dominion uses multiple layers of protection. For example, Dominion has developed an EMP E1 protected control house design standard. An independent third party tested the new control house configuration, and found it provides a significant measure of protection against E-1 effects.

In addition, Gardner noted, “wherever we can, control cables are installed underground, and are helically shielded as well. Finally, our storage centers and spare staging centers have EMP protection for critical components such as relays.”

Gardner underscored James Fama’s comments about the importance of partnership. Dominion, for example, has been partnering with its vendors to ensure that equipment is pretested by manufacturers.

Finally, Gardner noted that they have been building a new System Operations Center. “As the world has changed, you can’t operate our grid from an office park like it has been designed to, so we are building a new control center and we are designing that control center to contemplate the EMP threat.”
Chris Train, Director of Gas Distribution, National Grid, UK

Chris Train discussed the organizational structure in the UK for protecting critical infrastructure against “Black Sky Events.”

The process begins with the UK Government undertaking a national risk assessment study. Then it creates a National Emergency Plan, which sets out the roles people will need to fulfill in an emergency situation. Within the National Emergency Plan, there are Sector Resilience Plans, including one for the gas and electricity sector, which is led by the Department for Energy and Climate Change (DECC.)

Train went on to explain, “DECC then goes through an exercise of determining critical national infrastructure and the requirements for that critical national infrastructure.” An organization called the Energy Emergency Executive Committee (E3C) coordinates the implementation of the emergency plan across sub-sectors of the power industry: network operators, suppliers, generators and relevant government agencies.

The prime role of the E3C is to ensure coordination between government and industry, and critically important information flow “from the ground up.” E3C brings the key players together for regular scenario planning and training exercises.

Asked to sum up his presentation in one line, Chris Train replied: “A clear structure drives clear accountabilities.”

Chris Train stated that he wished to “thank NOAA and the Met Office for the work that they’ve done around forecasting CMEs, and the space weather forecasting.

“That has made a big difference in terms of our operation and our operational understanding, and has allowed us to do really clear exercises with operational people on the ground to make sure that we [preplan and] appropriately respond, as opposed to react, to such an incidence.”

‘‘If there’s one thing I think that we need to work on looking forward, it’s getting that balance [between regulation and market incentives] right, so that the right investments are made to ensure continuity of supply for customers.
Regulation tends to look backwards rather than forwards, and "isn’t very good at doing those Black Sky-type events." The market incentive of ensuring a continuous supply to customers, however, provides an important dimension for addressing emerging risk, and driving resilience planning efforts for a full range of projected hazards.

"If there’s one thing I think that we need to work on looking forward, it’s getting that balance [between regulation and market incentives] right, so that the right investments are made to ensure continuity of supply for customers."

“...In the U.K., based on a National Emergency Plan, critical infrastructure protection for the power industry is the focus of the Energy Emergency Executive Committee (E3C), which coordinates implementation across all power industry subsectors."
Water Sector
Paul Stockton, the session chair, introduced the shift to a focus on water, observing that “in a Black Sky event, with a catastrophic power outage, the very first, most imminent threat to public health and safety is likely to come from the cascading effects of the loss of electric power on the water and wastewater sectors.”

Chris Franklin began by emphasizing that a water utility’s ability to run its plants and pump water is wholly dependent on electricity. Moreover, he added, “the tolerance that we find customers have for being without water is extremely low.” This means that Aqua America must strive to maintain very high levels of resilience and reliability.

The obvious solution for ensuring backup electricity supply is preinstalled, large diesel generators at big water and wastewater plants, and back-up generators or strategically-placed spare generators that can be moved around for small, community water systems.

One challenge in implementing this model is the way in which some regulators interpret the “used and useful principle” – that customers may only be asked to contribute to recovery of the costs of plant that is currently “used and useful.” Some state regulators still do not consider emergency back-up generators to fall into this category, so that cost recovery is not feasible. This is an obvious deterrent to investing in such spare equipment.

Progress, however, is being made in working with regulators on this point. Now though, said Franklin, “In our most sophisticated plants with the best redundancy in more urbanized areas, we would have -- without power, given the use of diesel generators -- three days of water. Three days.”
One could improve the situation by storing more diesel fuel on site. But there are serious questions about whether the generators, which are not built to be permanent sources of power, could run for four weeks or more in the event of a prolonged electrical outage.

Power failure would also have a serious impact on wastewater facilities. If these plants were to fail, then the rivers and streams that serve as drinking water sources would soon become contaminated. Rapidly restoring power to waste-water plants is obviously critical.

Finally, Franklin contrasted the electric industry, which has undergone huge consolidation over recent decades, with the water utilities, which are still largely decentralized. Water utilities in the U.S. are mostly municipal and there are 50,000 community water systems.

This multiplicity of providers makes coordinated disaster preparation far more difficult. “So I’ll leave you with this thought,” he concluded, “that I think it’s safe to say that if we were to be really prepared for a major Black Sky event in the water utility industry, there would need to be a number of paradigm shifts – in preparation and in cost recovery.”

“...In our most sophisticated plants with the best redundancy in more urbanized areas, we would have -- without power, given the use of diesel generators -- three days of water. Three days.

“...If we were to be really prepared for a major Black Sky event in the water utility industry, there would need to be a number of paradigm shifts – in preparation and in cost recovery.
Dr. Peter Grevatt, Director, Office of Ground Water and Drinking Water, EPA

Peter Grevatt began by expressing his appreciation for the recognition, by summit speakers, of the interconnectedness of the power and water sectors as part of our critical lifeline infrastructure.

To illustrate the disastrous consequences of water supply failure, Grevatt recalled what happened when Charleston, West Virginia lost its water for five days in January (for reasons unrelated to the power sector). All schools and businesses closed and hospitals were forced to postpone surgeries and life-saving medical interventions. The cost of the water outage was estimated at $70 million.

A long term power outage, he pointed out, would be far worse, rapidly leading to a loss of water even for sanitation or fire suppression. “If you think about a long-term power outage, power equals pressure in many systems. You lose pressure, you lose sanitation, you lose fire suppression in addition to all the other uses. And you very quickly find yourself in a public health emergency.” Clearly, then, it is critical for the power and water sectors to work together closely to ensure the resilience of the power supply for the water and wastewater sector.

Grevatt noted that water has not always received recognition as being part of critical lifeline infrastructure. In this respect it is a victim of its own success. “People are so used to the idea that …you turn on the tap and a safe product comes out of your tap 24/7, 365 days a year.”

This level of convenience can lead people into complacency about the security of our water supplies. For example during Hurricane Sandy, some water utility requests for power were not rated as high priority by local state and federal authorities. In one case, a water utility saw its request for generator support turned down. As a result, it was unable to guarantee water supply to a regional hospital, creating an emergency in that facility.

The primary approach to addressing power security for water utilities is to work to ensure high priorities for sustained or restored power to water companies. “During large-scale power outages, particularly when critical power assets are damaged or destroyed, emergency operations centers...”

“Water has not always received recognition as being part of critical lifeline infrastructure… People are so used to the idea that …you turn on the tap and a safe product comes out of your tap 24/7, 365 days a year.”
and power companies are in the very difficult position of trying to prioritize who gets power first. And we need to continue to try and build a link so we can make sure that the water sector is among the first priorities to get power to avoid those kinds of public health emergencies."

The Water Sector Coordinating Council, in which the EPA participates, is a body that raises awareness of the vital importance of water supply at the Critical Infrastructure Partnership Advisory Council. The twin goals of involvement in this forum are, first, to make sure federal and state partners assign high importance to water in the event of an emergency; and, second, to help utilities increase their own power resilience.

Other activities aimed at helping water utilities increase their power resilience include a series of workshops on water and power resilience held since 2013. The EPA is also producing a “Power Resilience Guide for drinking water and wastewater utilities. This covers, among other things, communication with electric utilities, conducting power assessments to determine emergency power needs, as well as how to obtain, store, maintain, share and borrow emergency generators and possible funding mechanisms for resilience projects.” This represents an important foundation on which Black Sky preparedness must be built.

Thanking Grevatt for his presentation, Paul Stockton added that, in addition to considering the effects on water systems of a prolonged power outage, there was important collaborative work to be done in addressing the potential effects of an E-1 EMP pulse on the electronic systems that are integral to running modern water infrastructure.

“During large-scale power outages, power companies are in the very difficult position of trying to prioritize who gets power first. We need to build a link so we can make sure the water sector is among the first priorities to get power to avoid those kinds of public health emergencies.

“”In the current state of planning, a long term power outage would lead rapidly to a loss of water even for sanitation or fire suppression. If you lose pressure, you lose sanitation, you lose fire suppression in addition to all the other uses. And you very quickly find yourself in a public health emergency
Nick Santillo, Director of Operations Security, American Water Co.

Nick Santillo focused his remarks on the water sector Black Sky planning American Water has been helping to develop.

The first step, he explained, is to define minimum Black Sky service levels. This includes, for example identifying the most critical water system zones, based on an assessment of the vulnerability of the population served. The next step is to determine the minimum service levels appropriate for those populations.

The process is greatly improved if the utility can communicate with its customers and instruct them to reduce their water usage in the event of a Black Sky hazard. This would obviously enable the utility to stretch its resources far longer.

The next step, he said, is to identify the critical assets necessary to run the system at the minimal levels that were defined. This would not require all the utility’s assets to remain operational, and therefore not all facilities will need to keep backup generators or extra fuel and treatment chemicals.

The most critical priority, if possible, is to maintain enough drinking water for everyone in the community. That need is constant regardless of the nature of the threat we are defending against, he pointed out. Then a utility will need to define at what level of impact the community becomes unsustainable: “If we have X amount of customers over Y amount of time without water, what is the tipping point where we are looking at a mass evacuation for the community?”

Santillo stressed that wastewater services are vitally important here: “if you cannot flush, and we start to get sewer backups, now that incident grows, and your mass evacuations turn into another incident. The longer we can sustain that community, the better off we will be in the long run.”

“ If we have X amount of customers over Y amount of time without water, what is the tipping point where we are looking at a mass evacuation for the community?

“If you cannot flush, and we start to get sewer backups, now that incident grows, and your mass evacuations turn into another incident.”
Overall, the approach water companies will need to take is to look at defining where their utility will operate, given the range of choices for Black Sky service levels. Options run from potable water to a non-potable, ‘boil water’ notice. But [then we’re still] maintaining sanitation and we’re maintaining fire suppression. And then from there it would degrade to no water... our worst-case scenario, where we can no longer sustain pressure in the system. We don’t necessarily know what the full impacts of that may be.”

One of the lessons learned from Hurricane Sandy is that the longer the failure in the water system, the longer the recovery time.

For Black Sky scenarios, this means prioritizing sustained or rapidly restored electric service to water utilities will be vital. Achieving this, however, Nick Santillo pointed out, requires good coordination across sectors.

From a whole community perspective, “if we can look at it at a community level, we can educate from the water and wastewater sector into the electric sector and vice versa. Then we plan together, and that allows us to respond together.”

“If we can look at it at a community level, we can educate from the water sector into the electric sector and vice versa. Then we plan together, and that allows us to respond together.”

“Black Sky service options [will ideally] run from potable water to a non-potable, 'boil water' notice. Then we’re still maintaining sanitation and fire suppression.”
Session Two

“Where do we need to go?”

Imagining the Future of Lifeline Infrastructure Resilience
James Arbuthnot described developments in electronic infrastructure in the UK. He reported good news on two fronts. The first is that the security of UK electronic infrastructure is now led by the National Grid. The National Grid is one company, which makes coordination easier than in the US, though it also presents a single point of vulnerability. Arbuthnot praised the work of Chris Train at the National Grid in going a long way to address the UK’s vulnerabilities to space weather and EMP attack.

Arbuthnot suggested that the most immediate, serious threat to the UK grid now comes from cyber-attack, which is a constant, daily reality: “Our national grid is coming under cyber-attack every minute of every day,” he warned. “I want to hear no more of this phrase “low probability, high impact.” The impact is potentially devastating, as we’ve heard from many speakers today. But the probability is not low. In fact it’s not even probability. It’s constant, provable fact. The only issue is, will the bad guys get through?”

The second piece of good news was that the recent UK government budget had created a 1.5 billion pound security fund for any government department that wished to bid into it. The importance of this step was that it addresses the issue of “silos,” or departmental insularity and compartmentalization, whereby departments tend not to think beyond the borders of their specialized areas of responsibility. Arbuthnot described the security fund as being, in effect, “a virtual department of Homeland Security, without the disadvantages and costs that come with that, the empire battles and horrendous complication of organization.”

Arbuthnot ended his remarks by noting that while there was much more to be done by way of persuading people that the threats to critical infrastructure are real, actual and deserve funding, he felt optimistic about the progress being made.

“Our national grid is coming under cyber-attack every minute of every day...I want to hear no more of this phrase... low probability, high impact... The impact is potentially devastating... But the probability is not low. In fact it’s not even probability. It’s constant, provable fact.
This session reviewed the facilitated EPRO Black Sky exercise that took place the previous day, as the framework for the EPRO Executive Steering Committee meeting.

Speakers noted the crucial distinction in such exercises between “lessons learned” and “lessons imagined.” Many useful lessons were learned from Hurricane Sandy, but waiting to learn such lessons from a Black Sky event would, of course, be ineffective. Simulation exercises can help us imagine the lessons that need to be learned before suffering the event.

The exercise simulated an EMP attack on the eastern United States, leaving 100 million people without power, exploring the evolution of the event, and recovery operations, with two modules: today’s level of preparedness and then, later, assuming the much greater preparedness that could be reached in five years.

Characterizing top level lessons “imagined,” speakers referred to the ineffective, very poor recovery predicted in the first module, with its high projected loss of life. In the second module, with far more comprehensive preparation, improved Black Sky-focused electric sector resilience, emergency generation and fuel distribution planning and preplanned, broadly distributed and Black Sky compatible emergency communication were some of the most important differences noted. The projected loss of life was orders of magnitude lower.

A key lesson from the exercise: In a Black Sky event, services and personnel that we normally take for granted will, generally, not be available, including key lifeline utility response teams, at precisely the times when they will be most heavily needed. This was also projected as true for the emergency response community, which was seen as being severely impacted in the Module One scenario.

Implementing Whole Community Collaboration for Black Sky Hazards: The Challenge of Moving from Lessons Learned to Lessons Imagined
Avi Schnurr devoted his comments to providing more context to the feedback from the EPRO Black Sky Exercise that took place the previous day.

Expanding on the presentation’s title “Moving from Lessons Learned to Lessons Imagined,” Schnurr contrasted the successful “lessons learning” process that followed Superstorm Sandy with the impossibility of waiting to learn lessons from a Black Sky event. “As we look at Black Sky hazards, we will not have the opportunity to effectively learn from an event. If we wait until such an event to learn, that’s going to be just a bit too late,” Schnurr pointed out. “So how do we learn these lessons?”

Schnurr contended that these need to be lessons imagined rather than lessons learned. “We need to have tools that help us learn from them, without having these events happen.”

This is precisely the point of the Black Sky exercises – to imagine the event and, through doing so, to develop tools that would be needed to preplan and prepare for such an event – well before it occurs.

Schnurr expressed his hope that a growing number of lifeline infrastructure sectors and other partners would find opportunities to cohost such exercises, to help in developing planning for these severe scenarios.

“As we look at Black Sky hazards, we will not have the opportunity to effectively learn from an event. If we wait until such an event to learn, that’s going to be just a bit too late… these need to be lessons imagined rather than lessons learned.
Describing the EPRO Black Sky exercise scenario, Terry Boston began by highlighting the importance of the Black Sky exercise, pointing out the importance of planning for infrequent but severe events.

“We decided to test something we have no plans for,” Boston said. “Why exercise a severe scenario we haven’t yet seen? We have had three 1-in-100-year weather events in eighteen months. Now what’s the probability of three 1-in-100-year events? It’s a hundred percent. It’s already happened.”

The Black Sky exercise, he explained, is another example of an unprecedented scenario. In this case, far worse than recent weather disasters. “We looked at what if there was an EMP event that caused an outage to a hundred million people, and I gave an example yesterday: That the event that was tested over Kazakhstan in 1962 would have caused power outages from Austin to Boston.”

Terry Boston also added some additional detail on the exercise’s structure.

The exercise, he explained, simulated an EMP event that caused a power outage to around one hundred million people. He noted that such an event represents around five times the number of people affected in Superstorm Sandy, but with widely distributed damage pushing the outage into the long duration, “Black Sky” category.

The first module of the exercise, simulating a near term attack scenario limited to existing levels of preparation, resulted in “people freezing in the dark, without water, without power….and the communication system is down.” In addition, sixteen out of twenty interstate gas pipelines were projected to fail. Overall, this “Module 1” near term scenario was characterized by poor performance, with substantial societal breakdown and loss of life.

“Why exercise a severe scenario we haven’t yet seen? We have had three 1-in-100-year weather events in eighteen months. Now what’s the probability of three 1-in-100-year events? It’s a hundred percent. It’s already happened.”

The scariest thing that Paul Stockton wrote in EPRO1:…fifty percent of fifty six hospital generators failed during Hurricane Sandy.

We need an emergency plan for generators, emergency backup mobile generators. We need emergency transformers. We need a fuel supply path…we need an emergency fuel plan for the emergency generation.
Module 2 of the exercise simulated an EMP scenario taking place some five years later, in which levels of preparation were much higher. Critical transformers and other, selected grid assets were EMP-hardened, far more emergency generators were available and plans were in place for emergency fuel distribution.

This recalled, Boston said, what he referred to as “the scariest thing that Paul Stockton wrote in EPRO Handbook I: …Fifty percent of fifty six hospital generators failed during hurricane Sandy. The ones underwater failed first,” he quipped, and then others broke down due to the demands of long continuous runtimes, limited fuel, inadequate maintenance and a variety of other problems.

Module 2 also imagined that key public-private partnerships had been developed. “We had pre-certified electrical engineering teams,” he pointed out, “to come in and help.” A Black Sky-compatible Emergency Communications system was operational. In consequence, the results of this exercise module were vastly better. As Boston reported, “needless to say, we have much better response to this drill five years from now because we have done this planning. And we have two orders of magnitude less loss of life.”

And there were some particularly vital lessons “imagined,” he pointed out. “We need an emergency plan for generators, emergency backup mobile generators. We need emergency transformers. We need a fuel supply path…we need an emergency fuel plan for the emergency generation.”

“Referring to the previous day’s exercise, Boston reported, needless to say, we have much better response to this drill five years from now because we have done this planning. And we have two orders of magnitude less loss of life.”

“There were important lessons imagined from the exercise, Boston said. We need an emergency plan for generators, emergency backup mobile generators. We need emergency transformers. We need a fuel supply path…we need an emergency fuel plan for the emergency generation.”
Jonathan Monken reported how the Black Sky Exercise had helped people think about the many services and personnel we take for granted, that would not, without well-coordinated preplanning, be functioning after a Black Sky event.

“‘This is an action-based activity,’ he stressed. ‘We’re not doing this so we can write it in a binder... and then hopefully somebody knocks the dust off of it when they’re moving offices and says ‘that’s interesting.’”

Monken reiterated Avi Schnurr’s point that “a catastrophic power outage is a whole community event. Nothing can be handled in isolation.” Therefore it is critical for people to think about what they will do in a situation where availability of people, assets and equipment they regularly depend upon will be degraded and partly or wholly unavailable. And it is vital to remember, he said, “the effects of the response community being part of the impacted population.”

Monken gave as an example how, in just about any government emergency operations plan, the mass-care annex simply says,” Red Cross.” “Got it, it’s done, Red Cross will take care of it!” As Monken pointed out, such planning is useless if not pre-coordinated, and when volunteer availability in such a crisis may only be 10%.

Similarly, Monken warned against taking for granted the support and full-functioning of other sectors that were not represented in the exercise, and complacently thinking, “They’ve got this one covered.” His examples: Emergency communications, backup generation, fuel distribution and advanced logistics for utility-essential consumables. Moreover, he added, “if you have mass migration and public health issues compounding [the difficulty of] your efforts, your recovery will not happen, not only the way you expect it to, but it might not happen at all.”

Monken ended by looking forward to working with the stakeholders in the room on future exercises to address some of the vital questions that the Black Sky scenario planning had raised.
Panel 2
Opportunities and Challenges in Wisconsin

Panel Chair: Gen. Donald Dunbar; Adjutant General, Wisconsin National Guard

The State of Wisconsin is one of the most advanced in the US in its preparations to meet threats against electrical and other infrastructure. In this session, public officials and utility representatives described some of the state’s key resilience measures and planning.

A common theme that emerged was the critical importance of public-private partnerships. Public officials described their efforts to find out from utilities what they would need in the event of an infrastructure emergency. Among the answers that came back: Assistance with fuel, state border crossing, lodging and incident access, and information sharing. Speakers also drew a contrast between infrastructure protection at a federal and state level, with the smaller scale of available state resources requires an integrated response, where all key agencies deal with all threats.

Wisconsin utilities are also among the most advanced in protecting their infrastructure. One utility, ATC has already installed one of the first EMP/GIC blocking devices. Wisconsin’s emergency management agency and National Guard are also, now, building on the foundation of their well-practiced response mechanisms for floods and tornados, with new efforts to prepare plans for threats to infrastructure.
General Dunbar gave an overview of the State of Wisconsin National Guard’s emergency planning.

He contrasted threats such as floods and tornados where “we have really good, well-grooved response mechanisms,” with other threats such as long-term power outages induced by cyber or other Black Sky hazards, where the response, if limited to today’s preparedness, would be more like “trying to fly an airplane and at the same time trying to build it.”

Dunbar noted the important role of public-private partnership in protecting against such threats. In Wisconsin, the National Guards works with the electric utilities to identify vulnerabilities in the infrastructure and to share the task of protection.

At the state level, emergency response is integrated. “In the state of Wisconsin,” Dunbar noted, “unlike the federal government, we approach this together, not separately. The state government looks to FEMA for its physical response. They look to DHS for its cyber response. “We don’t have enough resources to do that in Wisconsin. It’s all hands on deck for all of our emergency response... So the same team that is working on physical response is worried about cyber response and physical effects.”

Well-coordinated emergency preparations, General Dunbar pointed out, are particularly crucial when considering a very severe, Black Sky event. “When you talk about losing power for weeks or months, somebody said you know, 150 years ago it wouldn’t have been an issue. It’s a big issue today when you think about everything from gas, filling your car, getting money out of an ATM. What would you spend the money on? Everything is just-in-time delivery.

“And if you lost that power, our system that is [ordinarily] so efficient would struggle. So I greatly appreciate the leaders in this room bringing this issue to the forefront.”
Brian Satula, Administrator, Wisconsin Emergency Management

Expanding on General Dunbar’s description of emergency planning in Wisconsin, Brian Satula began by noting that the state, like most others, recently went through a process called Threat and Hazard Identification and Risk Assessment (THIRA). One finding of the process: of the hazards reviewed, the threat for which the state is least prepared is a long-term power outage, in winter, resulting from a cyber-attack.

Satula discussed how to build on the emergency procedures in place for “blue sky days,” emergencies that are clearly within the organization’s capabilities to address. He noted that in comparison to these more routine incidents, exceptional “Black Sky” incidents will be characterized by three things. “There are too few responders. There's too few resources. And there are too many decisions to make.”

Satula described how his organization is “moving those decisions into the blue sky days so that when we get to the gray and Black Sky days we are ready for them.” To this end they are developing a seventy two hour, hour-by-hour comprehensive response plan, so that necessary processes and structures are in place. Workgroups on “Infrastructure and Private Services” and on Public and Private Coordination have been set up to further develop the response mechanisms for the fields of energy, communications, transportation, water and wastewater.

In engaging the private sector, Satula stressed that “the thing we did first is instead of telling private industry or the utilities what they can do for us, we asked them, “what can we do for you?”” Some of the answers that came back were “refueling, state border crossing…lodging and incident access, and information sharing.”
Mike Huebsch summarized the Wisconsin public Service Commission’s growing role in securing the state’s utilities against severe and extraordinary threats.

The commissioners receive monthly briefings on threats and emergencies, and “PSC staff have worked directly with several state agencies on planning, utility coordination and emergency exercise efforts. They have served in an advisory capacity for FEMA and participated in NERC’s GridEx II and GridEx III exercises. The PSC has also developed an Emergency Procedures Manual for dealing with utility disaster events.

In addition, Wisconsin’s PSC maintains contact lists of both utility operators and regional transmission operators. The PSC is in close contact with MISO, the Midcontinent Independent System Operator, Wisconsin’s transmission reliability coordinator, and which would play a lead role in implementing emergency procedures.

“The PSC has an important job during utility emergencies, including assessing information coming in from utility operators and assisting in state government responses when needed. Especially coordinating Wisconsin Emergency Management.”

Huebsch cautioned, “It is tempting for many in my state to believe that an average size state in the heart of the country such as Wisconsin is insulated from the natural and manmade hazards that threaten our electrical infrastructure.” Nevertheless, he concluded, Wisconsin is preparing diligently to meet those threats if necessary.

“Through diligent communication, cooperation, and preparation, Wisconsin will continue to strive to be a state, as referred to in the Electric Infrastructure Protection Handbook, where industry, government, and NGOs are partnering to strengthen the grid’s resilience against these extraordinarily severe hazards.”
David Wojtczak described how ATC, major electrical utility in Wisconsin and Michigan, is working to harden key grid elements and also to build grid resilience, particularly in the face of the EMP threat.

He referred to Wisconsin’s approach as treating EMP as a subset of an all-hazards approach, asking the question, “What do our systems look like if AC power is down for an extended period of time, in a wide [area] environment?”

ATC is already focusing on GMD (Geomagnetic Disturbance). It has installed measurement devices on transformers in key locations to improve situational awareness in a GMD event.

ATC has also purchased and installed one of the first EMP/GIC (Geomagnetically Induced Current) blocking devices. This is serving as a prototype, enabling ATC to gather data on the operating characteristics of the device, as installed in the grid.

Wojtczak also described his work examining the resilience of ATC’s emergency systems and identifying key vulnerabilities. For example, they tested how long the system operating centers could survive without power from the grid. The answer: about two days. Diesel fuel deliveries would be needed beyond the first forty eight hours after a disaster. ATC is now partnering with Wisconsin Emergency Management and National Guard to ensure diesel supplies for control centers.

Another key vulnerability is communications. How will situational awareness be maintained if the phone networks go down? Black start units are also an important area of focus, given that “typical substation batteries are good for about eight hours.”

Wojtczak ended by underscoring the vital importance of public-private partnerships. He noted, “We are already starting to see some synergies develop where we can call upon our friends in the public sector to help us get up and running, and supply much-needed resources to get the rest of the system up and running.”
Panel 3
Testing, Research and Development

Panel Chair: Terry Boston; CEO and President, PJM

The panelists in this session surveyed some of the testing facilities and recent research projects advancing our understanding of the effects of EMP and Geomagnetically-Induced Current (GIC). For example, Curtis Birnbach announced that AFS’s test facility can now create an extreme electromagnetic pulse, at a level of 250KV per meter. Idaho National Labs, Scott McBride told the delegates, has conducted tests simulating GIC, and assessing the impact to high voltage transformers. Dr. Sally Leivesley pointed to the importance of international cooperation in addressing new risks that often accompany technology advances.

Dr. Shlomo Wald, in his presentation, looked forward to the potential for new electric grid architectures, suggesting that a well-designed smart grid, based on local control of inputs and outputs through complex IT, has the potential to be inherently more resilient than traditional grid configurations. The next logical step to enhance resilience, he suggested, would be a smart energy and water network.
Curtis Birnbach described the advanced testing center that AFS has developed that can evaluate how equipment will perform under EMP conditions.

Explaining the AFS testing system, Birnbach stressed that "if you are going to build protective devices they must be tested under realistic conditions, and under the worst case conditions."

The 65,000 square feet testing facility will be able to do just this, among a wide range of other capabilities. Birnbach highlighted the importance of getting comprehensive test data. This can be important for two different considerations. First, to better understand vulnerabilities of existing equipment. Secondly, to gather comprehensive data on the capabilities of protective devices. AFS is building three EMP testing labs equipped with the most advanced testing and measurement equipment in the world, including EMP source equipment that can generate a pulse of 250,000 volts per meter.

Birnbach ended with a warning that the data we have on solar storms is not strong enough to support statistically sound predictions, suggesting that worst case impacts may exceed what has been observed in relatively modern times.

He pointed that, whereas “the earth has been around for four and a half billion years, we have maybe 100 years of good data. That is not enough to form a valid statistical basis.”
Dr. Sally Leivesley, Managing Director, New Risk Limited

Dr. Leivesley proposed developing a whole community research model focusing on maintaining energy supply to smart cities, and raised some of the challenges involved in such a project.

She pointed out the new types of risks inherent in the increased technological integration of cities: “Smart cities are becoming increasingly connected in their industries, such as we see in financial and other sectors….They’re connecting through the cloud. They’re creating every open pathway for a cyber-attack.”

The iconic nature of such cities makes them attractive targets. Leivesley suggested that two key goals in protecting cities should be not to cause an evacuation and not to cause a national economic loss. Preserving water supply is critical to achieving both these goals. These priorities would signal to any attacker that such an assault would not paralyze either the city or the nation.

Dr. Leivesley also spoke about the need for international collaboration to close off cyber pathways for potential attackers. This can help prevent nations having their systems and networks used to deliver attacks into another country.

She strongly reiterated the importance of grasping the interdependence of water and power sectors noting wryly, “you don’t survive very well otherwise. So water may affect you as well as you affecting water.”

In addition, she stressed the importance of educating and sensitizing the public to what would happen in a disaster, through education and exercises: “You must have the public working with you…(to) give you some breathing space and preempt some of the problems that you would otherwise have.”

Finally she noted the need for the widest possible threat monitoring, pointing out that a Daesh/ISIL weapons cache recently discovered in Egypt included a homemade drone to carry explosives under development: “Look at drones as a cyber platform or as an explosive platform, and you’ve got a lot of work to do.”
Scott McBride explained some of the testing of infrastructure components against EMP pulse that he has been involved with. The Idaho National Lab includes a test range compassing 890 square miles of high altitude desert. One area of the site is now known as the “Critical Infrastructure Test Range Complex.”

McBride described how over four years he has conducted tests simulating the Geomagnetically-Induced Current (GIC) caused by geomagnetic disturbances, and assessing the impact to power transformers.

One of the most significant results of the test was discovered when utilizing a particular electromagnetic pulse filter used by the Department of Defense. The filter is designed to protect against the E-1 and E-2 components of EMP. When they ran the tests with the EMP filter in the circuit, the total harmonic distortion increased from 55% to 75%.

As McBride expressed the conclusion for the tested filter: “what we found is that the filter designed to protect against E-1 and E-2 components of the electromagnetic pulse exacerbates the problem for geomagnetic disturbance.”

More tests are needed to understand this phenomenon, including on shell-form transformers, high-voltage auto-transformers and extra-high voltage core-form transformers. This must be the basis for sound science that can in turn ground sound policy and regulation.

“"What we found is that the filter designed to protect against E-1 and E-2 components of the electromagnetic pulse exacerbates the problem for geomagnetic disturbance."
Introducing Dr. Shlomo Wald, Terry Boston, the session chair, pointed out that Israel, Dr. Wald’s home country, is probably more advanced in its preparations to meet an EMP threat than any of the other nations represented at the summit.

Dr. Wald noted that since he was currently on sabbatical in Europe, he proposed to discuss the subject from a European standpoint. From that perspective, Wald suggested looking at EMP protection from the perspective of activities that governments are already pursuing and spending money on, particularly development of smart grids that may help protect against EMP hazards.

Explaining the concept of a smart grid and why it is relevant, Wald argued that the “big-is-beautiful” notion of an electric grid built on a hierarchy of utility system operators controlling the system for the consumers is outdated. Firstly, this kind of grid is inherently vulnerable; faults at a few key points may have disastrous outcomes. Secondly, the distinction between producers and consumers has given way to the concept of “prosumers.” Everyone can be either a producer or consumer at the same time.” Moreover, small producers today can be highly efficient, “so nowadays people are saying, small is beautiful.”

These factors have led to the smart-grid model of sophisticated IT layered on to the system so that operators can readily monitor and control grid input of a proliferation of small “prosumers.” The new grid will be based on the principle of local control. “That means that every site on the node will be able to decide how to operate, when to supply energy to the grid and when not to supply.”

This kind of grid will be much more resilient because “in the local control you can combine together analog and digital control and check on each operation...This is very good for cybersecurity and privacy protection.” So the move towards smart grids can enhance grid resilience and protection even if that is not the prime intention. Finally, Wald argued, “we should look not just for an electricity smart grid, but for a smart energy hub or an energy and water smart network...In this way we would be much better prepared for EMP.”
This session featured a range of perspectives from federal and state officials on next steps and challenges.

Assistant FEMA Administrator James Kish noted the federal government’s role is “not to decide who gets what” but to deliver support to teams in the field. One challenge arising from this is that the government does not directly support the private sector, but must find indirect ways to partner with, and be supportive of private companies.

Underlining this theme, the Department of Defense stressed that given the worsening threats against infrastructure, it is essential for the DoD to partner and work closely with the electric power grid, water treatment facilities and transportation networks to protect such sites.

Public-private partnership was also a theme of FERC Commissioner Cheryl LaFleur’s remarks. The Commissioner reviewed the coordinated process between FERC and NERC in developing recent standards for physical security, cyber-security and GMD.

As a key issue, a number of speakers referred to the issue of prioritization of resources in an emergency. This point, reiterated throughout the summit, was identified as an area requiring future work by each of their agencies.
Dr. Hoffman began her remarks with praise for the summit, an important resource for communication about “some of the priorities, some of the actions, some of the frustrations,” to help point the way to “where are we going next.”

“We’re going after prevention, …mitigation, and then response and recovery,” she explained. And in assessing those directions, referring to earlier presentations, she spoke of the growing body of available information to guide decision makers, addressing “the need for data and testing, and the research.”

“We need to test more components, more devices,” she said, and “to really think about the interactions on the systems.” In short, “a testing program is very important moving forward.”

Looking at the electric subsector, Hoffman referred to the full set of Black Sky hazards as important challenges: “EMP, GMD, cyber,…catastrophic earthquakes, hurricanes, or physical coordinated attack; all those are a priority to the industry. The question is how can we allocate the best resources in mitigating all those?”

Hoffman pointed to the broad coordination that DOE does with industry CEOs, with the Electric Subsector Coordinating Council, FERC and NERC on setting priorities, research activities and direction. In that regard, we need to “push forward on the highest priority activities that have the biggest cost benefit and impact to the sector.”

As examples of DOE’s work, Dr. Hoffman said DOE is investing in advanced transformers and transformer testing. DOE is also, she said, citing examples, moving forward with exercises that can help utilities “take a hard look at themselves and analyze their strengths and weaknesses.”

“EMP, GMD, cyber, catastrophic earthquakes, hurricanes, or physical coordinated attack; all those are a priority to the industry. The question is how can we allocate the best resources in mitigating all those?

“Fostering exercises is a priority for DOE, to help utilities take a hard look at themselves and analyze their strengths and weaknesses.
Hoffman emphasized the importance of data which could be used in mitigation efforts such as hardening equipment or in response and recovery operations. Further, she cited the push toward a “smart grid,” and other new directions and opportunities that will need evaluation. “Do we want … to have the ability to [expand the use of] microgrids or mini grids?” she asked, recommending discussion of costs and benefits. Such investments could then be evaluated, as we move forward with other “national imperatives and objectives that we have, such as carbon emissions reduction.”

Dr. Hoffman closed by speaking of the “deployment of renewables,” linking them to additional capability and flexibility in the grid, while warning that new technologies should be tested to make sure they do not jeopardize security.

Lastly Hoffman called for “transparent disclosure so that utilities can make cost-effective, accurate decisions ... and the whole of government can provide an effective response.”

“New investments and technologies should be tested and evaluated, as we move forward with other national imperatives and objectives such as carbon emissions reduction.”
Joshua Dozor, Acting Director, Planning Division, Response Directorate, FEMA (Federal Emergency Management Agency.)

Dozor began with his experience working at the National Response Coordination Center during Hurricane Sandy and realizing that the task was not just to respond to a hurricane but to respond broadly to the needs of a sector. Understanding a given sector, including the operations of the private sector and NGOs within it is vital if the federal agencies are to act and coordinate effectively with non-government entities.

Dozor corrected what he felt was a widely-held misconception about the role of the federal government in a disaster, “that the government decides who gets what.” Rather, he said, the federal government’s role is to deliver support to states and territories and to help coordinate the actors in the field. This role accentuates the need to understand clearly what the private sector and NGOs are doing so as not to interfere with their functions.

Another challenge is that the Federal Government does not provide direct support to the private sector. There are numerous indirect ways through which the government can be helpful, for example through waivers, regulatory relief, access controls, public safety and security. More research is needed on how to deploy these levers in the most effective possible way.

To prepare for future events, FEMA is preparing a Power Outage Incident Annex – “How do we respond to a massive long-term, large-scale power outage, whatever it may be, regardless of cost?”

He noted appreciatively that the EPRO handbook had been helpful in deriving some requirements that FEMA needed to meet, and also that the previous day’s scenario exercise had raised questions of prioritization that FEMA is also addressing such as “Do we work on the key population centers… do we work first on where we get the greatest percentage of infrastructure restored?”
Charles P. “Chuck” Kosak, Department of Defense, Deputy Assistant Secretary

Chuck Kosak spoke from the perspective of his work on counter-terrorism, and ensuring the continuity of DoD’s functions in an emergency. “Today’s asymmetric threat environment is unprecedented. And it’s worsening…” he said. “We have adversaries, nation states, as well as transnational terrorist organizations that have the ability now, and are continuing to increase the frequency of attacks here in the homeland. And their sophistication is increasing as well.” Moreover, he pointed out, the threat against domestic electrical infrastructure from physical or cyber-attacks is well known and worrying.

The use of social media and encrypted communications by terrorist groups are additional causes of concern to DoD, Kosak acknowledged. Hostile groups are researching vulnerable US sites, putting these up on the internet and encouraging their supporters in the US to execute attacks. Intelligence suggests that key infrastructure installations are possible targets. Therefore it is crucial for DoD to partner and work closely with power and water utilities, transportation networks and other sectors to protect critical assets.

DoD’s Mission Assurance Strategy, adopted in 2012, is one of the main initiatives in this area. It is based, he explained, on four pillars.

1. Identification
DoD identifies the most critical, mission-supporting defense assets. “A defense critical asset is something that’s so critical that a major operational plan or a contingency plan would fail if that asset went down,” he explained.

2. Assessment
DoD assesses and documents the risk to mission execution using an all-hazards approach. The risk of cyber-attack, for example, has become an increasingly important element of this assessment. This is a particular priority of Ashton Carter, the Defense Secretary. Some recent
3. Risk Management

This involves achieving an acceptable level of risk through additional planning. It may include building in redundancy to systems so that they continue to function after an attack, and remediation, which means investing in capacity to eliminate or mitigate a particular, single point of failure.

4. Monitoring

DoD establishes a common operating picture that encompasses risk management actions, the status of key assets and any changes to the potential threats or hazards. This also includes beginning to look at impacts. By understanding what’s going to be impacted and how, you can begin to plan how to restore affected systems. This common operating picture needs to be backed by a database, which is currently being developed and improved.

“For severe hazards, DoD’s Mission Assurance is based on four pillars:

1. Identification of the most critical defense assets
2. All-hazards assessment
3. Risk Management planning
4. Monitoring, using a common operating picture for risk, asset status and threats
Cheryl LaFleur, Commissioner, Federal Energy Regulatory Commission (FERC)

One of the main areas of FERC’s work is ensuring that there is a single binding set of safety and security standards applied across the whole of the high voltage electricity grid.

LaFleur focused her talk on three sets of standards, Cybersecurity, Physical Security and Geomagnetic Disturbance. These standards are developed in close collaboration with NERC, the North American Electric Reliability Corporation.

Beginning with cybersecurity, “Our cybersecurity standards are like the iPhone,” LaFleur quipped. “Right when you think you’ve bought your kids the latest and greatest and most expensive model, a new one comes along and makes it obsolete because it has more features.”

FERC is in its sixth version of cybersecurity protection standards, which now require some level of cybersecurity protection for all assets in the bulk electric system. Also FERC has proposed cybersecurity standards to apply to supply chain management in order to mitigate possible security weaknesses caused by industrial control systems purchased from vendors. While FERC does not have jurisdiction over vendors, it is encouraging utilities to exercise concern for security in their procurement processes.

Turning to physical security, LaFleur noted that in the previous year, the NERC worked rapidly to develop a physical security standard that passed through the whole regulatory process. This standard “requires owners and operators of bulk electric system assets to perform a risk assessment to identify those substations that are most critical when judged by the impact that losing them would have on the interconnection,” LaFleur explained. Once the critical assets are identified, “the owners have to evaluate potential threats and vulnerabilities specific to that asset: its location, geography and topology…and develop a plan to mitigate physical security threats.”

Finally LaFleur addressed the area of GMD standards. In 2013 FERC ordered the development of two standards on geomagnetic disturbances and their impact on the bulk electric system. The "Our cybersecurity standards are like the iPhone. Right when you think you’ve bought your kids the latest and greatest and most expensive model, a new one comes along and makes it obsolete because it has more features."
first standard, which has now taken effect, details operating procedures that could be carried out immediately when system operators heard that a solar storm is on the way. The second standard, LaFleur explained, “requires owners and operators to conduct assessments of the impact of GMD on their piece of the system and come up with mitigation plans for specified facilities.” This is challenging, she acknowledged, because so much work and research is still being done. However, she was pleased to announce that FERC had just approved the majority of the first draft of standards.

In closing, LaFleur reflected “that a lot of the work in the future is going to go into building in resiliency, building in redundancy, building the grid in such a way that it won’t be as vulnerable to cascades.”

“A lot of the work in the future is going to go into building in resiliency, building in redundancy, building the grid in such a way that it won’t be as vulnerable to cascades.”
Pamela Witmer, Pennsylvania Public Utility Commission

Pamela Witmer stressed the pivotal role of state Public Utility Commissions (PUCs). The Pennsylvania PUC requires all its utilities to have a security plan that is tested annually, and which covers physical security, emergency planning and response, cybersecurity and business continuity. Utilities are required to certify that they are continually upgrading their plans in the light of the annual tests.

The state legislature also required utilities to identify their mission-critical assets and develop special plans for protecting them, as well as requiring information sharing with the regulator. “It is very important,” Witmer emphasized, “to allow that free flow of communication back and forth between our regulated utilities and our agency.”

One particularly successful initiative in Pennsylvania has been the creation of the Critical Infrastructure Interdependent Working Group that brings all utilities together to share best practices and develop a common language. It was established following a communications failure with the power industry, after a large storm, in the aftermath of which telecommunications technicians had difficulty communicating with electrical industry people about the location of critical facilities.

Witmer acknowledged that, while the large utilities in the state have the human and financial capabilities to put sophisticated security plans and systems in place, “It’s our smaller and medium-sized business utilities that keep me awake at night.” Small, municipally run utilities are only partially within the PUC’s jurisdiction and “while they may not be targets for nation-states, they are certainly targets.”

To address this vulnerability, the PUC is developing a best practices guide that is directed at small and medium-sized utilities.

Witmer pointed out that “the human factor is one of our weakest points. So we are trying very hard to make sure that we’re living up to what we’re asking the utilities to do as well.”

“**It is very important to allow that free flow of communication back and forth between our regulated utilities and our agency.**

“**It’s our smaller and medium-sized business utilities and keep me awake at night…while they may not be targets for nation states, they are certainly targets of people who have way too much time on their hand.**
Session Three

How Can We Get There?

Whole Community Collaboration
As planning for Black Sky events advances in sophistication, new challenges come into view. This session surveyed some of the high level problems that need to be addressed.

Rep. Trent Franks began by reviewing political progress and the prospects for passing the Critical Infrastructure Protection Act in Congress, which would be the first US federal law dealing with the issue.

Paul Stockton and Jonathan Monken focused on some of the most critical challenges in emergency response and disaster recovery. These included establishing effective mechanisms for handling requests for assistance; developing policies and protocols for prioritizing and allocating resources among different requesting organizations, and better-identifying where necessary assistance will come from, especially where it needs to be procured from the private sector.

Speakers also emphasized the crucial importance for disaster response of sharing electric grid status information that already exists, and of developing a common set of data standards and trigger points for dispatching assistance.
Representative Trent Franks, Congressman (Republican, Arizona)

Rep. Franks opened by thanking all those involved in the effort to protect our societies from threats to critical infrastructure. He expressed optimism that the Critical Infrastructure Security Act had a good chance of passing in Congress and becoming law. This would “add large-scale blackouts to our national planning frameworks”. The Act would require the Department of Homeland Security to work with all relevant agencies to create a national strategy to protect the grid from EMP and GMD threats.

For the remainder of his talk, Rep. Franks considered the nature and seriousness of the main threats to the grid. He warned that according to NOAA scientists, it is not a matter of if the U.S. will be hit by a major space weather event, but when.

Turning to the EMP threat, Rep. Franks referred with concern to the 2010 Iranian military doctrine document “Passive Defense” which had just been translated by the National Intelligence University. The document emphasizes the importance of targeting critical infrastructure in warfare: “It references twenty two times to the use of EMP as a weapon to damage or disable the civilian grids of potential opponents.” Franks quoted from the document the Iranians’ conclusion that nuclear EMP is “an advanced, useful weapon in modern warfare.”

Rep. Franks also noted that the EMP commission testified that Russian generals had passed to North Korea plans for what they referred to as “Super EMP” warheads. North Korea, he reminded the audience, has already tested three nuclear weapons, in direct violation of its commitments to the United States.

In the face of these threats, Rep Franks underscored the urgent importance of adopting a national standard to protect the grid against worst case GMD or EMP events and to enable it to recover rapidly from such an emergency.

“\[This would be…the first time that American law will recognize the threat that electromagnetic pulse represents to our civilian infrastructure.\]"

“\[The 2010 Iranian military doctrine document … references twenty two times the use of EMP as a weapon to damage or disable the civilian grids of potential opponents.\]"
Dr. Paul Stockton, Coordinator, EPRO Executive Steering Committee

Dr. Stockton invited the Summit delegates to extend the discussion of cross-sector preparedness for infrastructure restoration and consequence management that had begun with the Black Sky exercise. He proposed to examine the consequences of cascading failure of lifeline infrastructure in a Black Sky event.

During Hurricane Sandy water and wastewater utilities were just about able to remain functioning. However, there are “unknown tens of thousands of water and wastewater systems that have no emergency power and it is reasonable to assume that in a Black Sky event some will fail.”

Stockton urged participants to “go one step further” and consider a more serious scenario than cascading failure: the situation where “the very same hazard that’s going to take out big components of the electric power grid is also going to severely damage or destroy components from these other infrastructure sectors.” So in the event of EMP, control electronics will also be destroyed in the water, wastewater, transport and communications sectors. How can power and infrastructure be restored and lives be saved and sustained under such a scenario?

Stockton proceeded to list some of the key functional capabilities that would be necessary to achieve this.

First, he emphasized, we would need a way of generating requests for assistance. In this area, FEMA and the Department of Energy have been working to learn the lessons from Sandy. Stockton stressed that this planning must go forward in close partnership with industry, “because industry is always going to lead the restoration of critical infrastructure.”

Stockton declared “I’m a Stafford Act guy” (referring to the 1974 disaster relief which places the onus on states to make requests for assistance). “Governors generate requests for federal support. They go to FEMA, which assigns federal departments as needed.” Industry needs to be integrated into this process, “because requests for assistance are going to come from multiple sectors simultaneously, at an overwhelming level in a Black Sky event.”

“Who gets what in a way that will save and sustain most lives, and really facilitate restoration of critical infrastructure?
Second, Stockton continued, we need to develop a way to adjudicate between and prioritize among different kinds of assistance. There will need to be criteria to determine “who gets what in a way that will save and sustain the most lives, and really facilitate restoration of critical infrastructure.” Developing such criteria for allocation of scarce resources will be tough but necessary.

Third, we have to figure out where the capabilities and resources for disaster response and reconstruction are going to come from. Stockton declared that his starting point is the principle enshrined in the Stafford Act, that FEMA provides mission assignments to government departments. However this leaves large questions open about what happens when there are gaps in the capabilities that exist or can be contracted from the private sector. This is a particularly pertinent question today in the cyber realm.

The final functional requirement that Stockton proposed was to prepare for “sustained operation of the system in the new normal, for months, for many, many months.”

Moving to discuss guiding principles of emergency response, Stockton asserted strongly that according to the US Constitution, “governors have primary responsibility for the public health and safety of their citizens. Not, repeat not the President of the United States...” We therefore need to build a system “that maps to the US Constitution.” Even if the crisis is a national security event, though DoD will have a role, primary responsibility rests with the governors. As a second guiding principle, Stockton reiterated the importance of building in the role of industry.

A final area to consider is how the planning is to be organized and coordinated across sectors. Is there to be a CEO level national coordinating council, for example? Summing up his talk Stockton declared that there are “big, big questions about what we would do in order to organize, in order to meet the functional requirements I identified in a way that respects the US Constitution and the leading role of industry in critical infrastructure.”

Governors have primary responsibility for the public health and safety of their citizens. Not, repeat not, the President of the United States...
Jonathan Monken, Vice President, US Operations, EIS Council

Jonathan Monken examined the interdependencies between different infrastructure sectors through the lens of information sharing.

Picking up on Paul Stockton’s point that there needs to be a consolidated system of adjudication for resource allocation, Monken raised the significant challenge of where we get the information on which to base educated decisions in such difficult cases. The information certainly exists, Monken averred: “I guarantee, I’ve seen the bunker, the PJM bunker...deep underground and heavily protected.” The problem is, how do we share the enormously detailed information on the grid that is collected by power companies like PJM to “empower these cross-sector relationships in order for them to make educated decisions?”

Monken recounted how, in his experience, even routine disaster responses may be inhibited by lack of basic information about the grid. A state or local government might set up an emergency operations center close to the disaster site only to find that grid coverage is poor in that specific area and there is no ability to connect to the grid. “With the access to the right data and right information, we can make those effective decisions to increase the efficiency of the overall response.”

Technically, the information can be accessed in conventional hazards, for example with the Eagle Eye System that scans the publicly facing websites of the power industry every 15 minutes. The important questions are how and with whom do you share the information as a basis for resource allocation?

The solution, Monken argued, must be to use a common set of data standards and trigger points. The unsatisfactory alternative is what Monken called “the CNN disaster” response where you have “a camera in front of a guy on Staten Island who goes, “Where is everybody? I’m here...I don’t have power to my house. I don’t have food. How come they’re not saving me?””

“With the access to the right data and right information, we can make those effective decisions to increase the efficiency of the overall response."
makers see the news and send help to Staten island, when in fact their need might not have been the greatest or most urgent. “

Monken stressed that “as it turns out, it’s not an [Information Technology] IT problem. It’s a governance problem. That’s what it really takes in order to be able to share that type of information, to make it useful and actionable.

A recent, multi-state earthquake exercise tried to identify the EEs or Essential Elements of Information that everyone needed to be able to see to make better decisions. It turned out there were three. “The number one request from everybody was power. Tell me where the power is. Number two, communications. I need to know if I can talk. Number three, transportation networks.” The area exercise led to unprecedented levels of information sharing between the participants.

“ It’s not an [Information Technology] IT problem. It’s a governance problem. That’s what it really takes in order to be able to share that type of information, to make it useful and actionable.
Panel: NGO Opportunities and Challenges

Fritz Wilson from Southern Baptist Disaster Relief and Keith Stefanelli from the American Red Cross explained some of the vital roles NGOs will need to play in recovery from a Black Sky event, and the interdependencies between the NGOs and other stakeholder organizations.

The disaster relief NGOs’ best known roles are to provide emergency food, shelter and comfort to affected populations. They also, however, have other less well known but highly valuable capabilities to contribute. Southern Baptist Disaster Relief’s volunteers include many retired engineers and power workers who could be deployed in an emergency, as well as thousands of ham radio operators who could play a critical role if normal communications channels are interrupted.

The NGOs also advocated drawing upon and building the natural resilience of the American people, by working to ensure that ordinary families are equipped with appropriate emergency supplies. By empowering the population to be survivors rather than victims, the speakers pointed out, they can be part of the recovery.
Wilson organized his talk around Avi Schnurr’s three opening questions to the summit: Where are we? Where do we need to go? How do we get there?

Starting with “where are we?” Wilson contended that voluntary organizations are “at the table” and they have high levels of capability. Wilson listed some of these capabilities.

For example, they have large numbers of retired engineers and power workers among their registered volunteers, who could be mobilized in a power emergency. In addition, their volunteers also included large numbers of ham radio operators; there are 5000 Southern Baptist volunteers with ham radio licenses. Communication, he pointed out, is likely to be one of the biggest problems after a disaster.

Another way a faith organization like Southern Baptist can help, Wilson offered, is by opening up houses of worship as points of distribution, information sharing and gathering.

Moving on to “Where do we need to go?” Wilson stressed the importance of preparedness. He cited the Mormon Church that has a program helping families to prepare kits to have ready for emergencies, asking them “what would you need for a three to four days outage. Or what would you need for six months or longer?” He noted that volunteers with disaster relief organizations have a fairly high degree of preparedness, through regular action in snow storms and hurricanes.

One challenge for NGOs that Wilson noted is the struggle to understand the impacts of a major electrical EMP or GMD event and what they would need to do in advance to protect their generators and other equipment. He appealed for help from partners in understanding this.

“The American people are resilient,” Wilson concluded. They are instinctively survivors. “Victims sit and wait for help. If we change our language and think of people as survivors and encourage them to be survivors, and equip them to be survivors post Black Sky event, they will be part of the recovery.”
Keith Stefanelli, Director, Emergency Management Coordination, American Red Cross.

The essential missions of a disaster relief NGO, Keith Stefanelli explained, are providing “shelter, food and comfort in some fashion.” That mission is the same irrespective of whether the disaster is a hurricane, earthquake or Black Sky event.

However, delivering shelter, food and comfort will be different in a Black Sky event. Stefanelli listed three primary challenges.

The first and primary challenge is communication and coordination. If they must operate without a Black Sky-compatible system, American Red Cross policy calls for personnel to try to “go back to the basics,” providing food, shelter and comfort. A related issue: How could assistance be coordinated from international NGOs?

The second challenge would be prioritization. “How do we figure out where we’re sending, human and material resources, in a multi-state, multi-region event?” To illustrate this point, he asked for a show of hands on who has a seventy two hour supply home emergency kit. Less than 50% raised their hands. Stefanelli pointed out that if a group of professionals in the field didn’t have that level of preparedness, one could hardly expect poorer and less-educated populations to go and buy a disaster kit.

The third challenge was transportation. Simply put, “if transportation networks are out, how are we going to get stuff from point A to point B?” American Red Cross recently deployed 400 volunteers to help out with flooding in Texas. How would volunteers be deployed in the event of a much larger disaster which also caused major infrastructure damage?

Finally Stefanelli made the point that the American Red Cross is also starting to see a role for itself in providing humanitarian support for workers in the utilities and their families in a Black Sky event.

“The essentials are… providing shelter, food and comfort in some fashion.

“How do we figure out where we’re sending people and resources, human and material resources, especially if this is a multi-state, multi-region event?”
Panel: Next Steps in Israel

Panel Chair: Dr. Udi Ganani; Vice President – Israel Operations, EIS Council

Industry and government representatives presented some of main developments in Israel's rapidly advancing preparations to address EMP and other threats to infrastructure.

Across a range of key infrastructure areas, substantial progress has been made. Israel Electric Corporation is preparing for full grid protection against EMP and GMD. The national water company is ensuring that it has enough functional emergency generators to handle a long duration, Black Sky hazard scenario, and the national gas company is protecting key production, storage and distribution nodes.

A number of the speakers stressed the value of international support and partnership, and praised the important work of EIS Council in helping Israeli decision-makers, along with those in the U.S. and elsewhere, to understand key aspects of Black Sky hazard protection.

Speakers also discussed the prioritizing process and criteria which led to Israel allocating resources to address these dangers. They alluded to Israel's unique situation as a country that faces many existential threats and can therefore serve as a kind of “laboratory” for evaluating, prioritizing and addressing some of the key threats that many Western nations face.
Dr. Udi Ganani, Vice President, Israel Operations, EIS Council

Dr. Ganani began by noting that, so long as Iran has an active nuclear program, EMP protection will be something that Israel takes very seriously.

He reported that in the last year, EIS council in Israel had made great progress in raising awareness of the risks of long duration power outages associated with EMP and other Black Sky hazards, and in encouraging key national organizations to protect critical infrastructure against such risks. These organizations include the Israel Electric Company, the Mekorot National Water Company, the government owned Net Gas company, and the Israel Defense Forces.

In addition, prominent academic think tanks, the INSS at Tel Aviv University, and the Begin Sadat Research Center at Bar Ilan University have begun to take an interest in EMP research. The translation of the EPRO handbook into Hebrew was a very helpful step in advancing understanding of the whole subject in Israel.

The Ministry of National Infrastructure, Energy and Water Resources has been a very willing partner, he said. For example, after just one meeting with the leadership of Mekorot, which falls within the Ministry, they put a team on figuring out how to ensure that their 470 emergency generators would keep working in an EMP event.

Similarly, the Natural Gas Group within the same Ministry (which will soon be responsible for 70-80% of Israel’s energy production) is working to ensure that their critical nodes are protected. Also, the IDF home front command is already thoroughly engaged in expanding protection of key infrastructure against potential rocket threats, while the IDF’s electronics and communications corps are working to enhance protection of the new facilities they are building in the South of Israel.

“So long as Iran has an active nuclear program, EMP protection will be something that Israel takes very seriously.
Dr. Naomi Etzion, EMP Committee Chair, Israel Electric Corporation

Dr. Etzion gave an overview of EMP planning in Israel Electric Corporation (IEC), the country’s electric utility.

IEC is beginning its work with simulation studies using dedicated software to calculate GIC (Geomagnetically Induced Current) distribution in the grid, to identify nodes at risk from EMP E3 or GMD.

“The next stage is to protect our transformers,” Dr. Etzion explained. “We would like to begin with the existing transformers. We will identify which should be protected based on transformer DC current thermal capability. For new transformers, IEC would like to write EMP protection into the product specifications.” For other equipment, she said, “Shielding protection and grounding improvements are the best solution for new construction. IEC would introduce cable entry shielding for control rooms, data centers and power stations.

Expanding on EMP E1 and E2 protection, Etzion noted that IEC already has lightning surge arrestors installed in many substations, likely also protecting against E2. Testing is necessary to determine whether it could withstand E1 and IEC is interested in recommendations.

Another important area of work is protection of critical installations, “defining methods and measures to maintain power supply to critical places,” for example through protection solutions for substations and power plants. Examination of how to build-in maintenance planning for high levels of equipment protection is also important. “If we harden some substation and then the man who did it retires, then how will we maintain it if we want to add an extra field in that substation?”

Finally, Etzion spoke about power restoration plans. IEC is developing guidance to staff on how to perform a detailed systems recovery after a blackout. There needs to be a storage facility for replacement equipment, and the storage facility itself needs to be protected against EMP. IEC has the budget to finish these pilot plans swiftly and to use them as a basis for building a long-term, professional, protection plan.

“The next stage is to protect our transformers. We would like to write EMP protection into the product specifications.
Yehuda Niv gave a top level Israeli perspective on electric infrastructure security. He noted that IEC is the overall authority for electrical infrastructure security, although the picture has become more complicated since Independent Power Producers (IPPs) began to enter the Israeli power market about a decade ago.

IEC has an emergency situation room that can communicate energy status updates to all the key state bodies. Since communication can be affected in an emergency, there are additional satellite communications in place between the government and emergency officers in the different major organizations. There is also a plan for coordinating public communications in an emergency.

“We live in Israel and in Israel we do not pray for miracles, we plan on miracles,” Dr. Niv quipped. Nevertheless, he pointed out, to ensure continuity of generation, all plants greater than 100 MW are dual-fueled, for security reasons. Natural gas and coal plants have substantial, onsite supplies. In addition to these local supplies, all gas-fired plants can also burn diesel, and most are connected to the national fuel pipeline system. This pipeline is connected to large reserves that would enable long duration plant operation.

All power stations must also conform to physical and local security, cybersecurity and operational continuity requirements. In addition, all hospitals have emergency generators that are tested regularly. The National Emergency Management Authority is working to ensure that all other vital industries and bodies also have emergency generators. One solution under consideration for this is mobile gas turbines of 10-25 MW that are carried to where they are needed on semi-trailers.

“We live in Israel and in Israel we do not pray for miracles, we plan on miracles. Nevertheless, he pointed out, all plants greater than 100 MW are dual-fueled.

“The National Emergency Management Authority is working to ensure that all other vital industries and bodies also have emergency generators. One solution under consideration for this is mobile gas turbines of 10-25 MW that are carried to where they are needed on semi-trailers.
Measures to protect the transmission system include extending the length of the grid line connections to introduce more redundancy into the system. There are also plans for wired bypass of the major substations “in case any of them are hit. This will provide reduced service, but continued operation.”

Cybersecurity is provided by IEC’s own cybersecurity operation, which is supervised by the National Cyber Administration.

“Measures to protect the transmission system include introducing more redundancy into the system. There are also plans for wired bypass of the major substations, yielding reduced service, but continued operation.”
Dr. Daniel Weinstock, Renewable Energy Association of Israel

Dan Weinstock summarized a study he did for INSS (Institute for National Security Studies) on infrastructure protection.

The study looked at four central threats.

The first threat examined was an attack by rockets and missiles. In the past, these have missed critical infrastructure targets. In the future, Weinstock warned, they are likely to hit. The second threat is natural disasters – earthquakes and tsunamis. The third threat is cyber-attack, and the fourth is EMP.

The bottom line findings of the report were that the Israeli electric grid is prepared for earthquakes, partially ready for missile attack and extensive cyber-attacks, and that EMP protection is progressing rapidly.

A key requirement for meeting all these threats, Weinstock stressed, is “we need reasonable – not perfect – protection of the power grid. We need fast recovery after severe damage. I was amazed yesterday to hear that according to the optimistic scenario, after twenty one days, ten million Americans will be without electricity,” he said. “If there are outages of forty five minutes in my hometown and actually all over Israel,” he quipped, “the mayor will be executed. Twenty one days without electricity is unimaginable.” We had better prepare to fix the grid - quickly - because we cannot plan for everything.

The main recommendations of the INSS report were to formulate a long-term national plan and to accelerate the transfer of the emergency division from the IEC to the Energy ministry. The report defined as a key, overarching goal, “reaching a situation where consumers will be able to maintain minimum essential function in a situation where there is no deliverability or only partial deliverability of electricity.”
Weinstock also strongly advocated expanding renewable energy generation as a way of enhancing grid security. The first advantage of renewables is that the primary energy source cannot be harmed. As Weinstock remarked, “Only God can stop the sun or the wind and last time I checked, God is on the side of the good guys.” The second big advantage is that renewables are inherently distributed and modular. Israel’s largest solar plant was hit by a missile while under construction in 2014. 1400 modules were destroyed, out of a total of 400,000, which represents only 0.35% of the field.

Weinstock also mentioned the potential of pump storage technology as a source of power that is resilient to attack. Israel is developing 1000 MW of pumped storage capacity. This is emblematic of huge advances now underway in storage technology, so that renewable energy sources with utility scale storage will soon be cost-competitive with other sources.

Finally, he noted the importance of estimating the electricity that a household can make do with in an emergency. In Israeli, this is assessed to be 5-7 kWh per day, about a quarter of normal consumption.

“Only God can stop the sun or the wind and last time I checked, God is on the side of the good guys.”
Jacob (Kobi) Wimisberg, Director, Strategic Cooperation and Assistance Division, National Emergency Management Authority (NEMA), Israel, Ministry of Defense

Kobi Wimisberg described how his organization, NEMA, took upon itself the task of raising awareness of the EMP threat in Israel, to help and advise decision-makers in allocating resources to protect against EMP. He expressed hope that Israel’s work on EMP protection would yield constructive lessons for other participants. “We need to be a community and we need to share with each other, and as such, I believe that every move towards strengthening one part of this community will strengthen the rest of the community.”

Since Israel is a country facing no shortage of threats, Wimisberg explained, the leadership is constantly faced with the challenge of prioritizing among these threats. “You can see, it’s like a beauty contest between the threats…they all say, I’m the most important, I’m the most dangerous. You must invest in me.”

The range and seriousness of the threats Israel faces represent a special case. The country has neighbors who literally want to destroy her. “It’s something that is existential and it’s something that is realistic. So to prepare, for us, is not a question of theory. It is a question of life.” This makes Israel something of a living laboratory “to conduct experiments on how to protect from different kinds of threats.”

Another distinctive feature of Israel is the isolation of its energy system. “We cannot trust our neighbors to help us in an outage or blackout, and so we have to prepare by ourselves and to set as a goal a standard of continuity of operation, not only of machines and technology, but of the society itself...The society, the public, and the institutions will continue to function throughout any kind of crisis, as regularly as possible.”

Given the myriad of serious existing threats, it was challenging to persuade senior decision makers to add EMP and GMD to the list. Initial reactions from ministers included, “I have a terrorist
as a threat. I have Iran somewhere in the background, and now you say the sun is an enemy?"

Another response Wimisberg encountered was “I don’t have enough money or resources to prepare the country for an event that I have no idea if or when it will happen.”

There are three main principles on the basis of which threats are prioritized in Israel. The first is the likelihood that the event will happen. The second is the severity of the event, meaning not just how many casualties is it likely to cause, but also how quickly can the country repair the damage and return to normal life. The third is the economic factor, which includes both the cost of preparing to meet the threat and also the cost of making an error by not preparing for an event that ended up happening.

The factors that led to EMP being accepted as a threat that Israel should prepare for were the potential scale of the damage and the fact that the leadership was not willing to accept the price of failing to prepare in the event that the threat actually happened. In addition, it was decided that EMP was not a very expensive threat to prepare for, both in terms of absolute expense and also relative to other threats that the country protects against.

Once the decision was taken to move forward, the next steps were to identify the relationships between the electrical grid and other critical infrastructure, principally communications, defense, cyber, health, the economy etc. to identify the most important institutions that need to be involved and then to develop the plan.

The process has involved a massive educational process within Israel and seminars, workshops and meetings to educate key ministries on long term outage risks, and on the EMP and GMD threats. International support and cooperation, with EIS Council’s cooperation, has been very helpful in this process. NEMA’s goal is to reach the point where a) Israel is prepared against EMP and b) EMP is recognized as a high risk on Israel’s map of threats.

There are three main principles on the basis of which threats are prioritized in Israel. The first is the likelihood that the event will happen. The second is the severity of the event, meaning not just how many casualties is it likely to cause, but also how quickly can the country repair the damage and return to normal life. The third is the economic factor, which includes both the cost of preparing to meet the threat and also the cost of making an error by not preparing for an event that ended up happening.
Panel
Lifeline Infrastructure – Opportunities and Challenges

Panel Chair:  **Terry Boston**, CEO and President, PJM

The work of both the Army Corps of Engineers and of NOAA directly relate to the challenges and opportunities faced by America’s lifeline infrastructure.

As explained by Karen Durham-Aguilera, Director of Contingency Operations and Office of Homeland Security for the US Army Corps of Engineers, the Corps has a unique role in the federal government, as the lead for responding to infrastructure problems in the National Recovery Framework. As the federal team designated, for example, to respond to the challenge of an extensive power outage, the Corps has the expertise and capability to integrate emergency generation in a critical facility.

For hazards like an extreme Space Weather event, this challenge can, over time, be mitigated by the work of NOAA, the National Oceanic and Atmospheric Administration. Dr. Louis W. Uccellini, Director, of the National Weather Service and Assistant Administrator of NOAA, pointed out that, like the Corps, many organizations – and especially power utilities – can benefit from advance warning of a severe space weather event that could precipitate a power outage. This makes the needs of such organizations, users of NOAA forecasts, particularly important to NOAA’s research and projections.

Durham-Aguilera described how reducing disaster risk, both the natural and manmade kinds, has become increasingly prominent among the Army Corps of Engineers’ many functions, especially since Hurricane Sandy.

Among the disaster-related functions of the Corps of Engineers is to serve as FEMA’s engineers providing public works and engineering in an emergency and its aftermath. “The Army Corps of Engineers is the infrastructure systems lead of the recovery framework” as Durham-Aguilera put it. “We work with the other agencies that have to do with infrastructure.” The engineering support functions include providing temporary electric power to critical public facilities, including dams, bridges and hospitals.

Durham-Aguilera underscored the importance of working closely with voluntary organizations and mentioned Team Rubicon a non-profit group comprised of mostly young combat veterans with whom the Corps of Engineers has a cooperation agreement. The Corps of Engineers has collaborative partnerships with a plethora of other organizations including the Department of Energy, the Department of Transportation, the American Red Cross, Americorps, Veterans Administration, the EPA and the US Coast Guard.

She noted that it is not part of the Engineering Corps’ mandate to define what counts as critical facilities in each area. This is the job of the states and local governments.

One especially relevant project that Durham-Aguilera singled out was an effort where the Corps of Engineers is working with the Department of Energy and FEMA to improve the generators that FEMA has stored at its numerous distribution centers. There is a particular emphasis on introducing larger generators that can power bigger areas and facilities.

“The Army Corps of Engineers is the infrastructure systems lead of the recovery framework”
John Madden began by acknowledging that he was part of a group that recommended what eventually became THIRA Threat Hazard Identification and Risk Assessment to Congress. He went on to describe the original recommendations which his group proposed which in several ways differed from THIRA.

Madden recommended that threats should be identified according to hazard lines and supply lines rather than by state, county or other political divisions. “It was about the hazard lines, the people all along a watershed, or a river, or a coastline, or a faultline, to look at the threats that face us and look at how we would go about it together, collaboratively.”

The process they suggest was first to analyze how things work; what is the supply chain and the interdependencies that make the very fine working system we depend on work so well. “What we wanted was something that started with how things work. How do seven million meals a day get into Manhattan? How does a gallon of gas reach into your car?” He went on to explain, “As we did that, then we wanted to say of that system that works very well, not perfectly but it works very well, what can go wrong? And then of the things that can go wrong, what are the consequences? And at that point, you’re educated enough to say now what do we do about it?”

He recommended that investments in buying down risk should “have a means by which you measure the effectiveness of that investment. And if it worked, you show that that helped to draw down a risk.”

Madden emphasized the importance of collaboration and recognizing interdependencies not only of goods and services but of authority. The various authorities need to recognize their interdependency and support each other. He spoke about interdependency of influence, “If
you do not control something, if do not own something, how do you use your influence in an effective and positive way to achieve the mutual benefit of both?” He also spoke of interdependencies of analysis. Situational awareness means getting relevant information “and having more than one view of what’s important and relevant helps us all understand.”

Summing up his remarks he said, “Work together is collaboration. Interdependency is a means by which we can have more success. And we do this through the partnerships such as what we have here. Partnerships are the process by which we meet our mission.” He ended by praising the EIS Summit as “a very successful forum.”
Nick Santillo, Director of Operations Security, American Water

Speaking in the final panel, Nick Santillo offered some broad observations from his perspective as a water company executive. First, he began, “I really appreciate being able to be brought into [coordination with] the electric sector.”

As one example of areas the water sector needs to explore, Mr. Santillo spoke about the need to begin looking at hardening to address emerging Black Sky hazards. “We do not protect against EMP generally today,” he said. Before participating in the EPRO ESC meetings, “EMP and solar weather were not really anything at a sector level that we were looking at. … So that’s something that I think needs to change in the sector.”

Nick Santillo went on to offer additional thoughts on some of the most important Black Sky measures needed within the water sector. For example, referring to emergency power, “We need to go back and look at our design criteria. Generally a water system is designed for one to three days of backup generation. That’s been a standard for years. When we start talking about extended power outages, such as a black sky event, that design has to be changed.”

Summing up, “I think we’re going to modify our planning and preparedness levels,” he said. “And that’s about keeping our systems operational, and doing what we can during a Black Sky event..”

Beyond that, it’s also essential to look at the supply chain for critical assets. “It’s really about fuel. It’s about chemicals, it’s about … transportation and roads. And then our employees. I was happy to hear with the NGO discussion about how do we support the employees’ families so that we can keep those employees at work and supporting us.”

This, he explained, highlights the importance of whole community planning. “We have to look at that community level planning, and we have to figure out as a sector … how do we participate in community level planning? And who is driving that planning?”

“EMP and solar weather were not really anything at a sector level that we were looking at. … So that’s something that I think needs to change in the sector.”
Making that happen will require thorough advance planning. For example, “What are our communication means?” he asked. When we have ... a Black Sky event, how do we communicate with each other? How does the water utility communicate to the electric utility, to the emergency manager? How do we collaborate?”

A critical next step then, is to start that cross-sector coordination process. “I've heard a lot of capabilities from different groups, from NGOs, from the Corps, and what I don’t necessarily know is how do we start a conversation at a community level to start that community planning? I think that’s a little bit of a takeaway. But we know that we need to be engaged in that process.” In that regard, he concluded, “on forums for collaboration, I think this is a great one.”