From: (b) (6)
To: Durkovich, Caitlin
Subject: FW: HEARING TRANSCRIPT 05-18-2016 HSGAC hearing re: critical infrastructure security
Date: Thursday, May 19, 2016 3:35:05 PM
Attachments: transcript - !DHS critical infrastructure security (HSGAC) 05-18-2016.docx

---

If you wanted to send the full transcript, please find it pasted below.

(b) (6)

JOHNSON: Good morning. I want to thank all of our witness for taking the time to join us here for your thoughtful testimony. I'm looking forward to the -- to the hearing.
Senator Carper is at a different committee hearing right now. He'll be joining us later and we have a number of members that also will, but are running behind. But I'd like to get started, be respectful of your time.
When I first took over chairmanship of this committee, coming from a business background as a manufacturer, I certainly found that developing a mission statement for any organization is pretty helpful. It directs the -- the activity of the organization. So working with Senator Carper, we developed a pretty simple mission statement: to enhance the economic and national security of America. They are inextricably linked.
This committee is really two committees in one: Homeland Security and Government Affairs. It's, you know, like the House Oversight Committee and the House Oversight -- Homeland Security.
On the Homeland Security side of the committee, we established four primary priorities: border security, cyber security, protecting our critical infrastructure, including our logical grid and then doing whatever we can to combat Islamic terror and other violent extremists to keep this homeland safe. We've been pursuing that mission statement, we've been addressing those -- those top priorities.
I guess it was about a year ago when we held our first hearing on potential threat of EMP. We had former CIA director, James Woolsey, we had Dr. Richard Garwin, who worked with Enrico Fermi. I believe Dr. Fermi referred to Dr. Richard Garwin as one of the few true geniuses he'd ever met. Some smart people, who even though some people consider, for example, the threat of EMP Holcim (ph), I asked point plank these individuals, do you think it's Holcim (ph)? The answer was an unqualified no, absolutely not.
Mr. Koppel, I truly appreciate the fact that you've written this book to raise public awareness of the vulnerabilities that we have with our logical grid. In the 2001 National Defense Authorization Act, they authorized EMP commissions, take a look at the potential threat posed by things like EMP and potentially geomagnetic disturbances as well. That 2008 commission established some recommendations that were to be undertaken by the Department of Homeland Security and the Department of Energy.
I'm going to take time to read them; they go A through O. I just want to take time to read what the 2008 EMP Commission recommended. A; to understand system and network level vulnerabilities, including cascading effects. B; evaluate and implement quick fixes. C; develop national and regional restoration plans. D; assure availability of replacement equipment. E; assure availability of critical communication channels. F; expand and extend emergency power supplies.
G; extend black start (ph) capability. H; prioritize and protect critical nodes. I; expand and assure intelligent island capability. J; assure protection of the high value generation assets. K; assure protection of high value transmission assets. L; assure sufficient numbers of adequately trained recovery personnel. M; simulate, train, exercise and test a recovery plan. N; develop and deploy system test standards in equipment. O; establish installation standards.

Now again, I realize that's kind of short bullet point form, but to me, those are some pretty reasonable recommendations. The secretary of the Department of Homeland Security and the secretary of the Department of Energy were basically -- it recommended their agencies start addressing these quick fixes, you know, these recommendations.
In our hearing, a representative of the Government Accountability Office basically reported that none of these have been done. This was again 2008 -- the results of a 2008 EMP Commission. Here we are in 2015, now here we are in 2016, none of this has been done. People are not taking this threat seriously and we have to.
So again, the purpose of this hearing is to lay out the realities, a very complex problem. Again, I'm not an electrical engineer, but we have got to start looking at exactly what the vulnerabilities are. We have to identify it, we have to define it, and from my standpoint, we have to take that first step in solving any problem, which is admitting we've got one which is the purpose of this hearing.
Now I do have a written statement for the record that I would ask to be entered without objection. And it is the -- and we'll wait for Senator Carper if he wants when he comes. We'll see if he wants to offer an opening statement.
But until that point in time, it is the tradition of this committee to swear in witnesses. So if you'll all rise and raise your right hand. Do you swear the testimony that you give before this committee will the be the truth, the whole truth and nothing but the truth, so help you God? Thank you.
Our first witness is Major General Dunbar. General Dunbar is Wisconsin's adjutant general. In this role, General Dunbar commands Wisconsin's National Guard and is responsible for emergency management. He also serves as Wisconsin's Homeland Security adviser, chairs the Homeland Security Council and is a senior state official for cyber matters. Previously, he served in the U.S. Air Force, the Washington Air National Guard and National Guard Bureau. General, thank you for your service and we welcome your testimony.
DUNBAR: Thank you, Senator. Good morning and good morning to members of the committee. Thank you for the opportunity to speak today.
I'm the adjutant general for the state of Wisconsin, and although I appear before you today in uniform, I want to stress that I am appearing on the behalf of the state of Wisconsin in a state status. I am not on active duty orders and no one in the Defense Department has seen, reviewed or approved my remarks.
I'm privileged to command Wisconsin's National Guard. As you know, the National Guard is constitutionally unique; it has two foundational roles. We're the primary combat reserve of the U.S. Army and the U.S. Air Force and the first military responders in the homeland. You mentioned my other roles, thank you for that. It's an honor to appear before the committee to discuss critical infrastructure.
Critical infrastructure is a shared responsibility. The federal government has a substantial role, as do industry leaders who generally own and operate the infrastructure. However, states have a leadership role as well. I'll touch briefly on our organization, our strategy and our efforts at addressing the threats to critical infrastructure in Wisconsin.
We did not create a separate agency to manage homeland security, choosing instead to rely on existing roles and responsibilities. Our governor created a Homeland Security Council, which includes representatives from state agencies and first responders who are joined by federal partners and industry leaders regularly to attend and participate.
Our homeland security strategy is updated quadrennially after each gubernatorial election and provides a framework to guide continuing efforts in preparation and protection of our communities and citizens. It also guides our investment of state and federal resources. The strategy seeks to ensure that our first responders are trained and equipped, that our critical infrastructure is safe and secure and that we continue to plan and prepare for emergencies and

disasters that may impact our state.
This strategy is our keystone document. It has four priorities: cyber security, asymmetric terrorist threat, catastrophic incidents and capability sustainment. Each priority has identified goals and objectives designed to be specific and measurable. Time doesn't allow for an in-depth discussion on all aspects of our efforts, but we are working on lines of effort to mitigate the threats to critical infrastructure. I'll highlight just a few.
In cyber security, we have developed at state expense a framework of five state cyber teams prepared to assist state and local government with cyber response. Three of these teams consist mainly of state and local professionals who by agreement have permission to respond when activated for a response.
We're developing a fourth team consistent with industry leaders, which will also be available to respond. And our fifth team will come from the National Guard. We currently have in the National Guard a computer network defense team that helps protect our portion of the DOD network.
The new team that we're building will be a computer protection team in collaboration with the Illinois Army National Guard. This team will be operational by the end of 2019, and although trained to meet the Army's military requirements, it is fully available for state active duty at the governor's discretion.
The Wisconsin National Guard is finalizing an agreement with several of our utility companies. Our agreement is aimed at information sharing of the potential for national guard physical support. We initiated this relationship after learning of certain real world events, such as the attack at Metcalf.
Wisconsin emergency management and the Department of Natural Resources partnered with our railroad commissioner and major rail lines and have arranged for a cash of critical foam to be stored regionally at no expense in case we have an oil spill and fire on our rail lines.
We've also revamped our hazmat structure, creating more versatile and regionally diverse teams that are strategically located consistent with population density and key lines of communication.
We are working with our public service commission and our utilities to understand better the threat to our electric grid and actively seeking ways to mitigate the potential affects. As an example, we're working with our public water and sewage utilities, all of whom have generator back up for their systems. However, all these systems require diesel fuel, and we're working hard to make sure we have a solid plan for delivery in an outage.
Another area we are discussing, although this is much more difficult given our utilities sophistication, is the physical back up to utility systems. I am no expert, but I took note of the recent cyber attack in the Ukraine which disrupted their power system. Clearly, Ukraine is not a system on par with the system in the United States. However, when they understood that the attack was a cyber attack, they switched to manual back up.
Based on open source reporting, this occurred after about six hours. The cyber network may yet still be infected, but the power disruption lasted only six hours. To my mind, that's a powerful lesson worth exploring and we're working with our POC to ask these questions of our utility partners.
Lastly, I'll mention that our national guard works closely with emergency management across the board in planning for and exercising our emergency plans. We're certainly not alone in this aspect, as the national guard across the nation has unique relationships with law enforcement, fire fighters, federal agencies and industry partners. Always ready, always there, we provide our nation's governors with a surge force that is highly trained and relevant across the domestic response spectrum.
I've submitted my written testimony for the record and greatly appreciate the opportunity to appear today and offer these brief remarks. I look forward to any questions you may have.

JOHNSON: Thank you, General Dunbar. By the way, your written testimony is entered in the record.
JOHNSON: Our next witness is Mr. Tom Farmer. Mr. Farmer is the chair of the Partnership for Critical Infrastructure Security Cross- Sector Council. Mr. Farmer works with the lead representatives for each of the critical infrastructure sectors and with senior government officials and coordinate efforts to advance priorities and capabilities in critical infrastructure protection and resilience. He also serves as assistant vice president for security for the Association of American Railroads.
Mr. Farmer?
FARMER: Thank you, sir, very much. Chairman Johnson and members of the committee and staff, thank you very much for this opportunity to address the priorities and cooperative efforts of the Partnership for Critical Infrastructure Security, or PCIS, Cross-Sector Council and critical infrastructure protection.
As the current chair, I am privileged to speak for a group of dedicated professionals across industries, who volunteer their time and efforts to take on leading and organizing capacities in their respective sector coordinating (ph) councils. Those forums formed in a national structure protection plan and enable industry to communicate and coordinate effectively with government.
It is the respective efforts of these professionals that merit attention, for they represent a sustained commitment for partnerships and action. Partnerships within their sectors, across sectors and with government. Their own (ph) statements submitted to the committee addresses a sampling of their efforts.
Their scope exceeds a time available for a fuller delineation here, but as I prepared for the hearing, I (inaudible) the chair of the Dams Sector Coordinating Council, well captured their scope in a delineation of his sector's activities, preparedness planning, exercises within the sector among dam facilities, cross-sector exercises with government officials and representatives of other industries, information sharing, cyber security guideline and tools that are developed in partnership with government, training and webinars focused on security awareness and preparedness.
Each of the sector's leads (ph) can certainly delineate very productive, pro-active efforts on behalf of their respective sectors. Across sectors, we are supporting these efforts by outreach and capabilities offered by government organizations. They include the Department of Homeland Security, the Federal Bureau of Investigation, the Office of the Director of National Intelligence, the various sector specific agencies and state fusion centers.
Their support in (inaudible) area is fundamental to enhanced and sustained effectiveness, including the structure protection. Areas like intelligence assessments, information sharing, risk assessments, resiliency assessments, tailored training and exercise programs, guidance materials for organizational sector-based preparedness planning and focused engagement on particular threats or security concerns.
This extensive body of work creates opportunities, opportunities that draw insights, that glean (ph) lessons learned to apply them practically in security posture and in protective measures.
A colleague in the Energy Sector Coordinating Council well captured the concepts with the phrase next level analysis, and priorities of our council emphasize this concept.
What we're talking about is knowing what we can know as thoroughly as possible, about using information proactively, about analyzing the wealth of experience gained by the expansive and effective work undertaken by DHS, FBI, other components. Particularly focusing on trends, on patterns, on indicators over current concerns.
Terrorism provides one example, investigations of attacks and attempts and disruptive plots reveal over and over again indicators that were experienced, observed, encountered that preceded the event. But their significance often wasn't understood, even if they were reported.

Similarly, active shooter investigations reveal similar behavioral indicators that preceded the events. We must and can learn from this adversity. Through analysis that highlights those recurring indicators of preparations, analysis enables professionals in industry and government to identify the opportunities for security measures and activities to make a difference.
We're very familiar with the see something, say something campaign. It works. But we can make it better. With this type of analysis, we can advance an informed see something, say something concept. Emphasizing those (inaudible) indicators and activities in preparations that have preceded acts of lethal and destructive violence time and again and apply that information in security training and awareness initiatives with employees across industries to inform their vigilance both on the job and in their home communities.
In cyber security as we contemplate the hundreds of on-site and virtual assistances (ph) that is provided by DHS and FBI in response to cyber attacks. As we look at the -- an excess of one million indicators of concern that have been disseminated by DHS to the private sector, opportunity emerges again.
For (ph) analysis that produces a cyber threat profile, a profile we can update on a recurring basis, to help organizations across sectors to understand what they're most likely to see in terms of how cyber threats materialize, one of those vulnerabilities that are so often exploited, one of those protective measures too often found lacking.
Now, as these analyses are produced, wide dissemination is essential. We need to make sure we have depth of penetration across government and industry. In the Cross-Sector Council, we have partnered with DHS to do just that, leveraging existing councils in government and industry to ensure that information in a timely manner reaches those who are best equipped to get it out to their respective constituencies.
We've also introduced the capability to share classified information and tested it on April 26th. Two components of the (inaudible) infusion center participated. And as part of that effort, we focus on ensuring that as the intelligence community produces products that are classified, that they also produce an unclassified tear line, a version that all who attend the briefing can take back to their organizations to inform vigilance and security measures.
The efforts of the respective councils are sound, they're proactive, no one is resting on laurels, we consistently seek opportunities to progress and our shared objective of enhancing critical infrastructure protection is obtainable.
I thank you very much for this opportunity to participate in this esteemed forum today.
JOHNSON: Thank you, Mr. Farmer.
Our next witness is Mr. Ted Koppel. Mr. Koppel is the author of the book "Lights Out". I've got a copy, unfortunately I don't have the cover. When I actually read books, I take it off. But "Lights Out: A Cyber Attack, A Nation Unprepared, Surviving the Aftermath". He is also a 42-year veteran of ABC News where he served as anchor and managing editor of the "Nightline" program from 1980 to 2005.
And I would point out this is actually my brother's book. He gave it to me. I would say he was a little alarmed. "Did you know this?" I was aware.
But Mr. Koppel, thank you for coming here. Look forward to your testimony.
KOPPEL: Mr. Chairman, Mr. Ranking Member, members of the committee, your late colleague, the distinguished Senator from New York, Daniel Patrick Moynihan, liked to say that each of us is entitled to his own opinion, we are not however entitled to our own facts. That observation, which seemed both sensible and the self evident can no longer be taken for granted. In a political climate where even the president's status as a natural born American citizen remains the object of doubt for more than a quarter of our population as he nears the end of his second term in office, in that climate, it will be difficult to settle the far more complex issue before the committee this morning.
Is the nation at risk of a crippling cyber attack against elements of our infrastructure in general

and against one or more of our electric power grids in particular? After more than a year of research into the question, I believe the answer to be yes.
Simply stated, the electric power industry is made up of 3200 separate companies linked in a network that both generates and distributes electricity. For the system to function, a perfect balance has to be maintained between the amount of electricity being generated and the amount being distributed. Only the internet is capable of maintaining that exquisite balance at all times.
The internet was never designed to be defended. The internet remains vulnerable to cyber attack. Evidence of that vulnerability is accumulating every single day in private industry, government agencies and in breaches of our personal data.
General Keith Alexander, the former head of the National Security Agency, likes to say that there are only two kinds of companies: those that have been hacked and those that don't yet know it.
Members of this committee are certainly familiar with the conclusion of our intelligence agencies that the Chinese and the Russians have already mapped and penetrated the systems that control our electric power grids. Iran is not far behind. Nations like North Korea and Syria are enhancing their cyber warfare capabilities. It is surely only a matter of time before a terrorist group unrestrained by any geopolitical interests acquires the capability to attack one of our power grids.
The problem, as Tom Ridge, our first Secretary of Homeland Security noted, is that ours is a reactive, not a preempted society. In the wake of the attacks on 9/11, 2001 the United States embarked on actions and expenditures that would have been inconceivable only a week earlier.
My message to this committee this morning is simple. The nation cannot wait for a cyber attack on the grid before making preparations for its consequences. It is my belief, and again this committee has access to more information on this subject than I, I believe that while the Department of Homeland Security has plans for dealing with the consequences of hurricanes, blizzards, floods and earthquakes, it has no discreet plan for dealing with the aftermath of a cyber attack on one of the nation's power grids.
The department's recommendations for each disaster are essentially the same: a two to three day supply of water for each person, a plan for families to meet at a prearranged point, a supply of essential medicines, flashlights and a battery-powered radio. A cyber attack against one of our electric power grids could deprive tens of millions of Americans of electricity for a period of weeks or even months.
I asked Homeland secretary -- Homeland Security Secretary Jeh Johnson what exactly he would be telling Americans on their battery powered radios after an attack that he was unwilling or unable to share now. He gestured toward a shelf carrying several white binders. "I'm sure there's a plan up there somewhere," he told me. I do not share the secretary's confidence.
We have neither the adequate food supplies to take care of those millions who decide to shelter in place nor the collaborative plans for the state governments to house and feed what could amount to tens of millions of internal refugees. If we began tomorrow, Mr. Chairman, implementing such plans would still take a couple of years.
I thank the committee for its attention to this critical issue.
JOHNSON: Thank you, Mr. Koppel.
Our final witness is Mr. Scott Aaronson. Mr. Aaronson serves as the managing director for Cyber and Infrastructure Security at the Edison Electric Institute. Prior to joining EEI, Mr. Aaronson served as a senior adviser to the chairman of the House Foreign Affairs Committee and Senator Bill Nelson.
Mr. Aaronson?

AARONSON: Thank you, Chairman Johnson and members of the committee. I'm glad to be here today to discuss security of the power grid. We appreciate you holding this important hearing and that Mr. Koppel chose this subject for his book.
As owners and operators of some of the nation's most critical infrastructure, we share his concern and the committee's to ensure that the grid is secure and resilient. From some of the headlines and movie script scenarios out there, you might think that we're not doing anything and being complacent, that there's a month-long -- a month- long power outage is inevitable.
AARONSON: If there's one thing that you take from my testimony today, it's to understand that the industry is doing an amazing amount of work at all levels all the time to defend the grid and to respond to an incident.
You have to remember we live and work in the communities that we serve. Our infrastructure is our most important asset. So we have every incentive to make security a major priority. Since these topics can be sensitive and even classified occasionally, we may not talk about them a lot in public. But don't take that lack of discussion for an inaction.
My written testimony has more extensive details on how the electric companies address threat. So I won't read that to you. But I do want to go through a little what we effectively call the three legs of the stool that make up security for the electric grid.
So the first leg of the stool is standards. The electric industry has mandatory and enforceable critical infrastructure protection or CIP regulatory standards for both cyber and physical security.
These are not lax, lowest common denominator standards. These are rigorous requirements that improve the security -- industry's security posture. Failure to comply can cost up to a million dollars per infraction per day. So suffice to say there is a lot of incentive to comply. But compliance does not equal security. Security is not a check the box exercise. If I do X, Y and Z I'm secured. No. You have laid a foundation for security.
The second part of what makes for full security, and the second leg of the stool, are partnerships. It has already been said, I think it was Major General Dunbar. Protection of critical infrastructure is a shared responsibility. In order to be prepared for an ever changing threat environment, industry and government are partnering at an extremely high level.
In addition to my role at EEI, I also am part of the secretariat for the Electricity Subsector Coordinating Council, or the ESCC. Along with the cooperative and public power segments of9 the industry, the ESCC is made up of 30 CEOs from across the sector.
These CEOs, CEO level, are meeting regularly with senior government officials from the White House, DHS, DOD, FBI, intelligence community and the Department of Energy, our sector-specific agency. They don't just meet to simply update each other or pat each other on the back and say we're doing a great job. They are setting a strategic vision for how we can improve the security posture of the industry, and by extension the nation, bringing together government and industry capabilities in a concerted way.
So the ESCC focuses on four major issues. I'll go through each of them briefly.
The first is deploying tools and technology. The focus here has been moving government developed tools to industry applications to improve situational awareness. And the best example of that is the Cyber Risk Information Sharing Program, or CRISP, which you can find in my testimony.
The second is improving the flow of information, making sure the right people are getting the right information at the right time. From classified briefings for executives to actionable intelligence for operators, government and industry are sharing threat information more often and more easily.
The third is coordinating with other sectors. While electricity's always described as the most critical of the critical, everybody relies on us, without water we can't generate steam or cool our systems. Without telecommunications we can't operate. Without transportation and

pipelines we can't move our fuel or move our equipment. There are a lot of ways to impact the grid short of attacking the grid.
To address these interdependencies, the power industry's actually working across sectors. And in fact, Tom Farmer and the nation's railroads have been great partners as we work together, for example, to move large transformers during incidents.
The last area of focus for the ESCC also happens to be the last leg of the stool. So we've got standards, we've got partnership. The last is preparations for response and recovery.
Simply put, electric companies have to be right 100 percent of the time, and the adversary has to be right once. Given those odds, preparation for an attack is just common sense.
First of all, we have a history of working together to restore power after an incident through mutual assistance networks where workers from unaffected companies descend on the affected company to restore power.
We also have robust spare sharing -- spare equipment sharing programs, including bilateral and multilateral arrangements. As well as a fully developed and legally binding plan called STEP, the Spare Transformer Equipment Program, that requires the sharing of large, hard-to-replace spare transformer restore during a national incident.
We exercise regularly. Of particular note is NERC's GridEx series which brings thousands of owners and operators and executives from across North America in the largest exercise of its kind. And now we are developing a cyber mutual assistance program to coordinate resources for companies affected by cyber incidents.
Bottom line is this. We are constantly working to manage risk, but understand that we can never entirely eliminate it. There isn't enough money in the world to protect against every threat in every location. But we are working to prevent incidents from having long term or devastating impacts.
We understand that the service we provide is critical to the life, health and safety of Americans. From CEOs to operators, the power sector has shown it takes this responsibility seriously, and is committed to constantly improving its security posture as these threats evolve.
Again, I appreciate the opportunity to be here, and look forward to answering your questions.
JOHNSON: Thank you, Mr. Aaronson. Let me start with you. You just talked about the STEP program, about these replacement, large power transformers.
In our E&P hearing, Dr. Richard Garwin, I asked him how many are critical. I mean what is the number of things that we really -- you know never -- large power transformers really need to protect. He gave me a ballpark. Somewhere between 200 and 700 of these large power -- is that -- would you agree with kind of around that assessment?
AARONSON: In fact I do. That's a fair assessment. Depending on what criteria you're using. Some place in there the number's going to fall.
JOHNSON: So how many replacements do we have for those that are basically ready to be moved into place in case either through kinetic attack or cyber attack or EMP or GMB (ph), those large powerful transformers are destroyed?
AARONSON: So the STEP program is actually governed by a nondisclosure agreement. So the specific number I can't give you. But I can tell you this.
Number one, we are sufficiently spared. Number two, outside of those spares that are dedicated through the Spare Transformer Equipment Program, other companies have, first of all, operational spares that they use for obvious reasons.
You will use a spare when you are doing maintenance on an active transformer. So you have that in place regardless. We have other ways of sharing equipment beyond just the Spare Transformer program.
JOHNSON: Let me ask you. So would I be able to -- with nondisclosures could I as United States senator find out how many we really have to satisfy myself that we really are covered?

AARONSON: I'd have to go back to the industry to see if we'd be able to breach the nondisclosure for that purpose.
JOHNSON: I'd appreciate that because the -- if you don't have spares, what is the length of time to replace some of these larger power transformers?
AARONSON: So the number that we've heard all the time is 18 month lead time. That's not entirely accurate. Under duress there are ways to procure transformers more quickly.
You also have to understand that there is a significant amount of excess capacity in the system. So when I say that we are looking to be able to operate under duress, we may go to a suboptimal state. One of the lessons that was learned out of Ukraine is going to a more manual operations.
So this rush to automation is great because it gives us wonderful efficiencies. But it also increases the attack surface.
So by diminishing the attack surface and looking at the ability to operate manually, the ability to operate sub-optimally, the ability to focus resources on more critical load, whether it be hospitals, first responders, military installations. Those are all things that because of this CEO leadership we are developing that capability.
JOHNSON: Based on reports my -- assumption's probably not the right word. But it sounded like the reason Ukraine was actually restored power six days...
AARONSON: Six hours.
JOHNSON: Six hours, I'm sorry, is because they actually had manual breakers, which we really don't have nowadays because we're more advanced. We have all computerized. Correct?
AARONSON: The answer is it depends. I always hate giving that answer. But the answer is it depends. In some cases there is the capacity to operate manually. In others we're going to need to continue to develop it.
JOHNSON: But -- OK.
General Dunbar, in your emergency planning, Mr. Koppel talked about in general we have plans to have provisions for two to three days. Is that pretty much what you have planned for Wisconsin in your capacity, in your responsibility?
DUNBAR: Our plans for long-term power outage taking care of the public. Quite honestly our goals is to try and keep the people in their homes so they don't add to the problem by a mass evacuation.
We do rely on the industry for the food stocks. It's a concern of mine because it's very efficient, as you know, and if something shuts down it quickly (inaudible) it out.
We do not have in Wisconsin a supply of MREs beyond what you would expect for the National Guard. And even that's limited because it's at the DOD level. It has those kinds of supplies.
JOHNSON: Mr. Koppel, I was pretty impressed with the level of reporting and the digging you did in your book. You didn't seem particularly convinced. You seem to have certainly asked some pretty hard questions. And you weren't getting particularly good answers.
Do you agree with Mr. Aaronson that we're probably sufficiently backed up in terms of large power transformers?
KOPPEL: Well first of all, I'm in no position to agree or disagree with him because I don't have access to the numbers either.
What I've heard and what was in a Department of Energy report back in 2014 is that the number of large power transformers is quite literally in the tens of thousands. So I'm frankly a little bit astonished at the notion that we're only talking about, what did you say, 250 or so?
AARONSON: Two hundred to 700.
KOPPEL: Two hundred to 700. I think, a, the number is greater. B, I think we're dealing with a problem of unique pieces of equipment that cannot easily be interchanged.
And C, Mr. Aaronson sort of dismissed the notion that it takes up to 18 months to get a new

one. But most of these large power transformers are not constructed in the United States.
The majority, I think about 70 percent of them, are constructed overseas. And by the time you order these and have them built we're talking about pieces of equipment that weigh between 400,000 and 600,000 pounds.
It takes at least a year and up to a year-and-a-half to order a new one and have it delivered. And even once you get it to the United States, delivering these things is incredibly difficult because they tend to (inaudible) distress pieces of infrastructure like failing bridges.
JOHNSON: Mr. Farmer, in your testimony you were really concentrating a lot -- and this is of course good -- of things, you know coordination and communication and planning. That type of thing.
But can you talk about what we've actually done to prepare and protect? You know I mean physically. What have we done in terms of infrastructure to improve our survivability and improve our ability to stand the power grid back up?
FARMER: Well, I'm not specifically qualified to discuss and detail the electrical sector. What I can say, though, is that there have been very productive partnerships fostered through the Cross- Sector Council that enable industries to identify interdependencies and then work in concert to enhance their resiliency, to enhance their preparedness, to address concerns.
Scott Aaronson addressed in his testimony the cooperation with the railroad industry on preparations to move large transformer equipment should we be in a situation where due to some form of damage a transformer is taken out of operation. And the electrical industry, electrical sector approached our industry.
We've worked in close coordination to do a number of things. One is to have preparedness plans in place for railroads to move the equipment. We've identified the types of railcars that move the equipment. We maintain a current inventory of where those railcars are. We have worked with the electricity sector through exercises the last two years.
FARMER: Each year the railroad industry holds an annual security exercise. In that exercise we take actual events and take them to another level through realistic terrorism and cyber scenarios to stress our industry security planning, to stress our procedures, our decision making, our actions to address concerns, our coordination with government.
We've integrated an exercise the last two years scenarios involving damage to large power transformers, and in the electrical industry calling upon our industry for support in their movement. So this inventory is maintained by a group called Rail Link. It provides informational technology support to our industry.
We can generate and update inventory within a matter of minutes to identify where the cars are specifically. And during the exercises, railroads' operational leads have worked with representatives of power utilities on what the transportation plan would look like. We're confident that provided notice of a need that within a matter of hours we would have a rail transportation solution in place.
JOHNSON: OK. Thank you, Mr. Farmer.
Senator Carper?
CARPER: Thanks much, Mr. Chairman.
I want to apologize to our witnesses. You know we serve on a number of committees. And one of my committees, Environment and Public Works, was holding what we call a mark-up today, voting on a number of bills, several of which were mine. And I needed to be there to defend them.
And so I can't be in two places at once. But I'm pleased to be here. And thank you all for joining us today, really important subject.
I'm going to go ahead and use this time to give an opening statement. And then maybe we'll have a second round for questions and I can ask some questions of all of you.
But obviously what we're discussing today is of importance. It was in Delaware and I know it

is in the other 49 states, the security of our critical infrastructure.
When we talk about critical infrastructure we're not just talking about the grid and supply of electricity, but also the dependability of our water, even our financial system that supports our economy. Unfortunately, our electricity and water utilities, as well as our banks, are risked every day in a number of ways.
We've heard a lot lately about the criminals and terrorists targeting them online. But these critical services are also at risk due to any number of other hazards such as violent storms, earthquakes, even failure due to aging and underinvestment.
Fortunately, Congress, our administration, private sector have been hard at work to address vulnerabilities in a number of these areas. And we've asked the legislation in the recent years to help make our critical infrastructure more secure, more resilient. I'll mention just a couple of examples.
In 2014 members of this committee worked for many months to enact legislation to reauthorize and enhance something called a Chemical Facilities Anti-Terrorism Standards Program, affectionately known as CFATS, within the Department of Homeland Security. This program was our front-line defense against terrorist attacks against companies that stores, manufactures and process hazardous chemicals.
That same year, 2014, our president signed legislation from this committee to enhance the Cybersecurity Center at the Department of Homeland Security that works with critical infrastructure owners to prevent and respond to cyber attacks. In that same year we also gave the Department of Homeland Security the authority that it needed to hire the best and brightest cyber talent that's out there.
Just last year the president signed cybersecurity legislation the chairman and I, and almost every member of this committee played a key role in drafting. The crucial new law makes collaboration between the federal government and companies grappling with cyber attacks easier and faster, while protecting privacy concerns.
And this year we're working hard to ensure proper implementation of these and other laws.
We're also working to streamline and strengthen the office within the Department of Homeland Security that helps protect critical infrastructure.
I've never cared for agencies that have a name that doesn't really explain what they do. And we have one that we ought to call it NPPD. It's the National Programs Protection Directorate that's within the Department of Homeland Security. Doesn't tell you a whole lot about what they do. But what they do is important.
And as the chairman knows, my staff and I have been working with Department of Homeland Security on legislation to streamline this office so it can better partner with industry. We do this in part by elevating its cyber functions and making sure that physical and cyber threats to our critical infrastructure are assessed jointly so that the left hand knows what the right hand is doing.
We also want to change the name of the agency so people have some idea what they actually do, and to name it the Agency for Cyber and Infrastructure Security. Doing so will make it clear that when there's a problem with vulnerability in the electric grid or some other piece of critical infrastructure there's no question about who in the federal government can help, should help. And who can be held accountable when things go wrong and maybe singled out from time to time when there's praise that's due.
As we know, unfortunately bad things sometimes happen. And the important thing is to be prepared for that when they do. So I want to credit the men and women at the Department of Homeland Security, including the NPPD, and elsewhere for the hard work that they do to ensure our critical infrastructure is secure and resilient.
As one example of this important work the department conducts an on-site assessment and incident response for dozens of critical infrastructure companies every year. When we talk

about critical infrastructure, especially systems we cannot afford to lose even for a few minutes, this means building resiliency into our policies and practices.
Today's discussion about critical infrastructure reminds me of one very promising technology that is already happening to make our country more resilient to electric grid outages.
I was a naval flight officer for a number of years during the Vietnam War. When we weren't over in Southeast Asia we were stationed in Moffett Field Naval Air Station. And we basically shared that large air station with NASA.
And later on when Moffett Field was closed due to active duty purposes, some private sector companies came in and partnered with NASA and they've done all kinds of amazing things. And one of them is called Bloom Energy.
They manufacture fuel cells. Do the -- basically some of them manufacture in California. Do a lot of the R&D in California. But they also manufacture fuel cells in Delaware.
These stationary fuel cells do not require additional transmission capability to move electricity to the end user, meaning reliable electricity can be provided even when the electric grid goes down. And innovative solutions like this can help us be a lot better prepared for a variety of threats in the future.
And with that, I want to thank you all for coming. And I look forward to asking you in a few minutes a few questions. Thank you so much.
JOHNSON: Thank you, Senator Carper.
Senator Peters?
PETERS: Thank you, Mr. Chairman. And thanks to our panelists for your testimony today. This is certainly a very important topic, especially given the changes we're seeing in our society in terms of being interconnected in ways that are difficult to fathom.
And critical infrastructure operational, whether it's dams and bridges, grids, will all be connected through the Internet of Things. And we're looking at millions and millions of objects all connected on this elaborate grid, even to the point that our electric toasters will be on the grid. So any sort of attack on the grid could have, without question, a catastrophic impact on society as we know it.
Let's talk about a variety of things. Hopefully we'll have some additional time if possible to talk about some of the cyber issues and physical attacks.
But one that I want to take a little bit of time on is an area that I focused on as a result of my work as a ranking member on Space and Science Committee, as well as being on the Homeland Security Committee. And this is an -- this is something that we know will happen that will be potentially catastrophic to the electric grid if we're not fully prepared.
And those are space weather events where you have mass coronal ejection from the sun, which sends particles to us here on earth. It has the impact of compressing the magnetic field if it is large enough, which puts huge pulses of electricity through pipes, through electrical transmission lines, can blow up transformers and shut down vast parts of the grid for the country.
We know it will happen. It happens regularly. Some of them are very large. The largest one that we know of is the Carrington Event, which occurred in 1859.
We didn't have a whole lot of electricity back then. We only had telegraphs. But all the telegraphs went down in the country. They were all shut down as a result of this event.
The sky lit up. Folks thought it was daytime. They got up, started making their eggs and breakfast. It was the middle of the night because the sky was illuminated so brightly from the storm.
Our scientists believe the storms occur about every 150 years, they hit the earth. That last one was 150 years ago. So it's been a while since we've seen it.
We did monitor a storm of that magnitude in 2012 that missed the earth by seven days. So we came very close to having one of that magnitude as well, which will have a significant impact.

And so I've been working with my colleague, Senator Booker, who's on both of the committees with me as well. We've introduced legislation to provide additional research and data working with NOAA and NASA and all of the federal agencies, including the Department of Homeland Security.
And the numbers are quite concerning. And the fact that Lloyds of London estimated that if we get hit with another Carrington type event, the impact to our economy would be anywhere from $600 billion to $2.6 trillion, that's what we're looking at as an impact from one of these storms.
And we could see up to 40 million Americans without power. And as we've had this discussion talking about the large transformers, some of that could be a year or two. You could have 40 million folks, particularly along the Eastern seaboard, which is particularly susceptible to these kinds of solar events.
So just think of New York City without power for a year. That's not a good thing. New Jersey without power, which is why Senator Booker's been very engaged in this as well, a very concerning thing as well as for me in the state of Michigan. So we have to do a better job of preparing for that.
And so I'd like to ask Mr. Aaronson specifically, what sort of research and information do you believe electric utility companies need from us as we're working on legislation to provide more information, more advanced warning? What specifically do you need to prepare for this event? And how do you view it?
AARONSON: Well, so it's specifically what you said about your role on the Space and Science Committee. Notice is incredibly valuable when it comes to space weather.
We actually have a geomagnetic disturbance, GMD, standards in place. The North American Electric Reliability Corporation, because it's something we have known for quite some time could happen, has developed GMD standards which dictate operational protocols to mitigate the impact of a serious coronal mass ejection.
So a big part of that is, again, advanced notice from an operational perspective so that operators can take action to shut down certain systems in a graceful way, let the solar flare do what it's going to do, and then be able to start back up again using something that's called -- it's been discussed already, black start capability, which is basically starting the grid from scratch.
Black start standards are in place. GMD standards are in place. And additional notice from some of those geostationary satellites that give us, I think right now we get about 15 minutes notice. Increasing that even to 30 minutes would be invaluable.
PETERS: Well, I mean that's an important factor is that we may not have a lot of advanced notice. Our prediction capabilities for space weather are not as advanced as they should be. Folks have described it to me that we are where we were with hurricane predictions in the 1930s when it comes to space weather events.
PETERS: So we have a long ways to go. Where we may know something is happening, we don't know the magnitude. We don't know where it's going to hit. And hurricanes have significant impact on us, but a $2.6 trillion impact to the grid that shuts down everything obviously is -- is a major concern.
So if you had just a perhaps 18 hours notice, is that enough time? And what sort of protocols are in place if -- if NOAA or whatever the relevant agency is at the time as we work out some of these protocols, say we think this storm is coming. This may mean you'd have to shut down vast amounts of the grid in the United States.
AARONSON: So, another thing to note is this is something that, as we've said, we've known about or known could happen for quite some time. And in fact, there have been examples of impact because of GMD, particularly at the higher latitudes where the impacts are more pronounced.

So, there have been examples of GMD impacting the grid, but for minimal amounts of time. You will note that telegraph lines from the 1850s are significantly different than the infrastructure we own and operate today.
Mr. Koppel, during his answer to Chairman Johnson, was talking about the fact that there are literally tens of thousands -- 45,000 actually -- substations in the United States; 55,000 in North America. With that comes an exceeding amount of redundancy. So the reason that the number is closer to between 200 and 700 of the most critical substations is because those others represent excess capacity and redundancy throughout the system.
It is -- it is inaccurate to say that a single geomagnetic disturbance would have a universal and unilateral impact across the entire grid. So really what you do have to look at is as much notice as possible to take those operational protocols to shut down the grid, to prevent -- to prevent damage. Understand that in certain instances like that, you have what's called voltage collapse, which means that the systems fail safe. And then we are again able to restart it through black (ph) start capabilities.
And then, obviously, the redundancy and ability to move transformers around in order to restore power should a particularly damaging geomagnetic storm impact the grid.
PETERS: Which -- and I appreciate that comment, which I think highlights the fact that we need to do a whole lot more research into these storms. Because you mentioned, it does not have uniform impact across the entire grid, but you need to know where it's hitting. And that's where -- I made the analogy to hurricane research, you need to know where it's going to actually hit in order to prepare -- not the whole eastern seaboard, but those particular areas where you think it's path.
So the same thing for this research for space weather, to make sure the resources and the coordination are available for all of the federal agencies -- NASA, NOAA, et cetera -- to provide that information to you. But I also wanted to make sure that I highlight the fact that these -- the critical infrastructure are these major transformers, as Mr. Koppel talked about as well, who are -- for the most part are not made in the United States.
They're made in Europe is the primary manufacturer for them, and a large space weather event could not -- has the potential not only of destroying the transformers that exist in the United States, but actually destroying or at least shutting down the facilities that manufacture the transformers in Europe at the same time. A large storm would actually shut down the manufacturing. So then you couldn't even make these until first you repair the entire -- the entire infrastructure to even create transformers before you make them and then ship them to the United States.
So this is something that I look forward to continuing to work closely with the utility industry. I know you're focused on it. I know this is an issue that you have been following as well. But we've got to make sure these protocols are in place and we're really thinking this through.
AARONSON: And I can say fairly unequivocally that helping to get more advance notice and increasing domestic manufacturing capacity for transformers are two things that the industry would be happy to work with you on.
PETERS: Great. Thank you.
JOHNSON: Senator Peters, first of all, thank you for that line of questioning.
I wanted to just follow up just briefly. In a previous hearing, we were told I think by testimony about $2 billion annually damage because of other types of solar events, OK? So this is just happening all the time. But the massive ones, like Carrington Effect, is something -- you know, (inaudible) greater.
Mr. Aaronson, I just have to ask you, if the protocol gave warning, 15 to 30 minutes so we can shut down systems, who's going to make that call? Who -- I mean, who's going to make that call under a massive (inaudible) disturbance that could -- that nobody knows, you know, how many of these transforms could be affected. Nobody knows. Who's going to make that call to

shut them off-line -- take them off- line so those -- you know, those effects don't go through those wires (ph) and destroy those -- those large power transformers that cannot be replaced?
AARONSON: So grid operators are tightly aligned. We have talked about the fact that it is -- there are 1900 entities that make up the bulk of the electric system. There are regional transmission operators and so on.
JOHNSON: Who makes the call? Who makes the call we're going to shut them all down in 30 minutes?
AARONSON: So...
JOHNSON: In 15 minutes.
AARONSON: It's not a simple as just cut the power. That's not how this is going to work. But there is, again, this shared responsibility among the sector...
JOHNSON: Who makes the call?
AARONSON: ... to be operating this -- I don't know the answer to that question.
JOHNSON: I think that's what Mr. Koppel's talking about.
Let's see here. Senator Tester?
TESTER: Thank you, Mr. Chairman.
I want to thank you all for your testimony. We're going to talk about a little different kind of infrastructure since you're here, General Dunbar. That is the infrastructure of our ICBM forces. It has been -- well, currently we have got -- (inaudible) that flyer (ph) personnel out for protection purposes. We're looking to get some Black Hawks in a couple of years, earlier if we can. But in a couple years at the latest.
There have been some that have suggested that maybe we ought to use the Army National Guard for defense of our ICBMs to make sure that they're secure. Fire season aside, that -- if we use them for that, they won't be available for fire season. It seems like the fire seasons are becoming more and more significant every year in Montana. It doesn't seem like it, but in fact, they are.
From your perspective, what kind of training needs to go in -- or are they already trained for National Guard soldiers to be able to protector our ICBMs?
DUNBAR: Senator, thank you for that question.
So let me start by again making clear for the record that I'm here speaking on behalf of the state of Wisconsin as a National Guard officer, not for the United States Air Force. Very important federal mission and I would not propose that I speak in any way for the United States Air Force on that issue.
In terms of the National Guard, the National Guard's advantage to the country is at a -- is a highly-trained Army and Air Force to do certain missions for the Army and the Air Force, and from that comes a surge capacity for all kinds of missions. So in California and other states, National Guard members have been used to fight fires both on the ground and in flying helicopters.
I can talk in the state of Wisconsin that we have our Black Hawk pilots. Not all of them, but some of our crews trained to fly Bambi Buckets to help put out those fires that you talk about. In terms of moving personnel from point A to point B, it's pretty much square within a Black Hawk's mission that most crews have that capability in their wheelhouse.
In terms of whether it's a good idea, I would -- I know you know this, sir, but the National Guard is a state military force until we're mobilized for active duty, so if the Air Force needed the Guard to do that mission, then they could ask for volunteers. If the governor thought that it would interfere with the state's response to firefighters, the governor could push back and say, "I'm not going to authorize volunteers," and then of course the federal government could trump that, as it always can...
TESTER: Bingo.
DUNBAR: And say we're going to be on active duty.

TESTER: OK. Just curious, I mean, we can solve this whole problem by getting the Black Hawks in quicker, but it's -- that's not within your purview.
I want to talk to Mr. Aaronson for a second about transmission and the threats on the grid, I should say.
Is that -- and excuse me if it has been asked already. But is that -- is that threat mainly in transmission or in generation?
AARONSON: So, I guess I'll answer it this way. The threat is mostly in transmission. Generation -- there are so many generation assets.
TESTER: Yeah.
AARONSON: Blending (ph) electrons to the grid. Those are assets we want to protect, but transmission is where really where it's at.
TESTER: Yeah. And so is this -- is this due to our reliance, because I know nothing about, quite frankly, how this whole system works. So, we're starting at zero.
But is this due to our transmission reliance on the web? Or why -- why should we be concerned about this from a terrorist standpoint?
Or are we talking about bombs blowing stuff up?
AARONSON: Well, so, a lot of answers to that question.
TESTER: Yeah.
AARONSON: First of all, you're not alone, Senator, in not knowing lot about how the electrical grid works. Most people just figure you turn on the light switch, and the lights turn on.
TESTER: As long as they turn on, that's good.
AARONSON: And that's our goal, too. We don't want you to think about all of the things that are happening behind it.
TESTER: Yeah.
AARONSON: There are a lot of threats to the grid. And you know, from we say like from squirrels to nation states. And frankly, there have been more blackouts as a result of squirrels than there are from nation states.
TESTER: Right.
AARONSON: The various threats, the reason the transmission matters -- think of transmission as the -- the...
TESTER: I know why it matter, truly, because my lights don't come on without transmission if we don't connect it all up.
AARONSON: That's right.
TESTER: The question is, is why is transmission a target? Is it because of the internet, or is it because of something else?
AARONSON: It is because it is a soft target by definition. There are 35,000 substations in the United States. There are long lead -- lines are everywhere.
TESTER: OK, you're right. And by the way, those substations have been around a long time.
AARONSON: They sure have.
TESTER: And we were -- in conflicts in World War II, there were substations, conflicts in Vietnam, there were substations, conflict in the first Gulf War there were substations.
Why now? What is different than Vietnam? Why should be concern now? And we never heard anything about it in the late '60s?
AARONSON: The threats continue to evolve. You can look at geopolitical situations. You can look at the fact that we used to be...
TESTER: OK, so the threat level is greater?
AARONSON: ... superpower. The line that we were a nation with friends north and south, and bordered by ocean.
TESTER: Right. OK, so the threats have raised is what you're saying.

AARONSON: That's correct.
TESTER: The threats of people who are doing damage to the homeland have raised, and they weren't necessarily -- Ted, do you agree with that.
KOPPEL: No, Senator, I don't. What has changed is that the electric power industry has become deregulated.
We now have 3,200 companies. I'm as much of a novice at this as you, so I've reduced it to a very simple analogy.
TESTER: As we like.
KOPPEL: I want you to imagine a balloon that has 3,200 valves. And half of those valves are letting air into the balloon, and the other half are letting air out of the balloon. As long as you maintain a perfect equilibrium between the amount of air coming in and the amount of air going out, your balloon stays inflated.
Too much air in, the balloon blows up; too much air out, the balloon collapses.
The electric power industry is made up of 3,200 companies. You have to maintain a perfect balance between the amount of electricity that is generated and the amount of electricity that is used. Too much electricity in, you've got a problem; too much electricity out, you've got a problem.
Only the internet has the capability of maintaining that exquisite balance. There was no internet back in the days of Vietnam. There was no internet back in the days of World War II. You are dealing with a total different kind of electric power industry.
TESTER: That's right. And I appreciate that answer, because I was -- that's what I had surmised and -- and -- and I will tell you that technology has done -- just -- technology has done a lot of really good stuff for efficiencies and predictability and dependability.
I come from agriculture and interestingly enough I had a guy get on my combine -- I actually still drive my combine. I don't have a GPS unit on it. And I had a guy get on my combine last year and he says, how do you know where to cut, because you don't have a GPS unit that's telling you where to harvest.
The point here is this. If we still -- if we want to talk about preemption, I think you have to run back and try to figure out how -- how you can still manually control this stuff. And if it's impossible, as you may be correct, Ted, the internet's the only way to control it, then we've got to figure out different ways to do this.
I will tell you that -- the -- the comments about tens of millions of refugees, which is probably true -- I mean, we've got to work on preemption because I don't see how we ever deal with a situation like that.
It amazes me flying into this city how we feed people in this country, much less how we would feed them under a catastrophic situation.
(UNKNOWN): If I might, I'd like to add a little bit of context to what Mr. Koppel said because he raises an important point about the fact that it is 3,200 -- 1,900 that take up the bulk electric system.
First of all, it is not controlled by the internet. We are talking about operational technology, supervisory control. These are not internet facing.
So yes, it is true that digital overlay is exceedingly helpful in providing these efficiencies, but it is not uniquely capable of keeping the grid operational.
Think back to just 20 years ago. We operated the grid for the better part of a century without digital overlay. There is the capacity to keep electrons flowing regardless of having supervisory control...
TESTER: That -- you are correct and the only thing I'm saying is if the threat has emerged because of the internet then we need to go back to that system as a fail-safe.
(UNKNOWN): And -- and we are. People who looked at what happened in Ukraine at the end of last year as this eye-opening experience for the electric sector, it was not eye-opening. It

was something that we were aware could happen and have been preparing accordingly.
TESTER: Yeah. Thank you. Mr. Chairman.
DOLD: And I want to point out is highly sophisticated so the use of the internet, those operators thought the systems were working properly when they weren't and I think the greatest threat is taking that the step further and having the destruction of those large power transformers that we can't replace -- that takes something from a six hour shutdown to days and weeks and months and that's what I continue to be concerned about.
My primary concern is -- structuring in some way, shape or form from various threats of these large power transformers. And again, I think we're -- I think you're minimizing what that is. I know you're just trying to be a little too soothing in this process.
Our next -- Mr. Portman -- Senator Portman.
PORTMAN: Thank you, Chairman, and thank you -- and Senator Carper for holding the hearing. Incredibly important issue.
I want to talk about something that -- is specific to a threat to our infrastructure and that's the increasing evidence out there that we have ran somewhere that has infected, not just individuals' computers but to commercial systems and I've -- recently had the opportunity to get a briefing from the FBI on this and I noticed that they sent out something on their website just a couple weeks ago warning people -- there's a unique, I suppose, warning out from the Canadian government and our government right now on -- on ransomware based on some information.
PORTMAN: To me, this seems to be a growing problem and yet it's underreported because my understanding is a lot of companies are not eager to talk about their ransomware payments. For those who don't follow this, this is when you have an infection in your system and you find your system has been encrypted to the point that it's blocked.
And you get a notice saying if you play this amount of money during this time period, and sometimes there a clock that shows you apparently what your time period is. We will pull the malware off and you'll be able to operate your system.
There's been some unfortunate instances of this, that have gotten a lot of attention. One was the Hollywood Presbyterian Medical Center in L.A. earlier this year, for weeks they had to shuttle their patients to other facilities because they were locked down with a malware problem.
So I guess my question, probably is best to you Mr. Farmer because you're here as chair of the Partnership for Critical Infrastructure Security. I have, I'm sure you've seen this report, the ICIT, which is the Institute for Critical Infrastructure Technology, issued this report and it's headline is kind of jarring.
It says 2016 will be the year ransom ware holds America hostage. Maybe the title of your next book Ted? But, so Mr. Farmer could you tell us and I know this date is difficult to come by because again it's not always reported.
But based on what the FBI has said and based on this report and based on some of these specific instances that have come to the media's attention. What's the nature of the problem? Is it in fact increasing dramatically as some say? What are some of the ways in which we as legislators could be more effective in dealing with it?
FARMER: Thank you sir for that question. I do think the problem is expanding and the FBI is attentive to it, the DHS is attentive to it, the reflective of that the media coverage highlights those cases where ransom ware has not only had an effect but actually worked. And I think like anything else, so long as the tactic is working the interest in pursuing it is going to expand.
On reporting, there's two avenues to focus on in terms whether incidents get reported. Often an infected organization will report a matter to the FBI as a law enforcement concern. The FBI will handle that matter through it's investigative procedures with the affected entity.

Whether it gets shared more broadly is a determination that entity might make with it's sector partners, with DHS but there's a lot of reporting that which has informed the FBI's efforts in providing these awareness bulletins in terms of entities affected by this, trying to deal with the problem and seeking law enforcement assistance.
So I think on that side you've got a lot of good reporting. And because the manner the FBI handles investigations that generally with the affected entity. Now because of the FBI's experience, and I give the FBI a lot of credit here, they've done a great deal of work in taking what they're learning from these law enforcement investigations.
Stripping out the indicators of the affected organizations and then publishing for wider dissemination, guidelines, advisories and in particular papers that focus on indicators.
One of the things we focus on in the cross sector council is we're not necessarily interested in who the perpetrators are, that's investigative information that's not necessarily important to us. What is important is the tactics, how is it that these events are taking place?
And in particular, how is the intrusion occur on to the affected networks? And the focus of our cyber security priorities collectively is on that aspect. What can we learn from all that work the FBI does in its investigative efforts? As I mentioned earlier, from all that assistance that DHS provides in terms of onsite work with affected organizations and sharing indicators.
Let's take that next analytical step and understand better how these events happen. So what makes it to the media is the effect. The computers are no longer accessible, the hospital can't get to their records so the effect makes it. But what is far more important from the cyber security prospective is how did that happen?
And I think as Mr. Koppel can point out, just from the work that he did in connection with his book, too often the means of intrusion are apparently simple. And there's a lot of work that we can do based on that next level analysis, understanding what those tactics are that are used most often, understanding what vulnerabilities are most often exploited, that can be hacked in advance.
Understanding what protective measures when that support is extended or found lacking? I'll give a comparative example. In Australia, they're equivalent to the United States Computer Emergency Readiness Team, did analysis of times when the Australian government, I think their signals director in Australia, had to provide assistance to private entities in Australia affected by cyber attacks.
And that analysis found that 85 percent of those cases, that if four categories of protective measures had been taken those attacks never would have materialized as they did.
And so we look at that from the U.S. prospective, we credit DHS and FBI for that expansive work and we say lets take that next step of analysis and build a very good cyber threat profile, that we compare with the cyber security framework issued by the NANS (ph) Institute of Standards and Technology.
And sectors can look at that and say, for organizations of varying sizes, this is what the threat looks like. These are what the vulnerabilities are the most often exploited. These are the protective measures that we need to pay attention to and marry those with objectives of the framework.
(UNKNOWN): Mr. Farmer, I would say with all do respect to that analysis that's been done and the information that's out there. I'm looking at a bulletin, right now, that's on the FBI website, it's tips for dealing with ransom ware threat, and yet it's dramatically increasing as I understand it. And as this report says, and I think you confirm that.
FARMER: Right.
(UNKNOWN): So despite our ability to understand how these ransom ware attacks are happening and the situation that's out there, it's expanding. And I think one reason it is, from what I understand, sometimes the ransom ware folks are asking for relatively small amount of money. Small enough that frankly they are not being investigated, so let's say $10,000. I'm

told that's kind of the sweet spot.
My view would be we need to up the enforcement of that and investigate all of them. Because it's sort of the broken windows, I guess, analogy on the policing side. You can't let some of these ransom ware happen and then second how do you encourage people to report? As you're saying some do report on the law enforcement matter, some don't typically if it's a relatively low level.
And then the final thing, and this is where I think Ted Koppel has done a great service, is talking about what restrictions are there that we could help with? Both at the regulatory level and the legislative level to allow people to protect themselves better. The great example that I have in some research that my team did, was hospitals that are told under the HIPAA rules they have trouble defending themselves following these very tips that are being laid out.
And I think you wrote something about actually an Ohio incident where there was a brown out in Ohio and some regulatory issues affected the people were able to defend themselves. Is that accurate? Or am I missing -- --
FARMER: No, I think you're accurate sir in terms of the nature of the threat. You're accurate in terms of the expansion. I do believe a similar wide spread publication of investigative actions and successful prosecutions that result in serious penalties for this behavior would be helpful, as a deterrent factor. I will say this though, I'm not -- I don't agree --
(UNKNOWN): So going after people more aggressively who are participating in this and increasing the fines or the criminal penalties.
FARMER: Increasing the criminal penalties but also taking that step too of insuring that those sorts of penalties are well known. So again, the focus of attention is on what happened in the particular event, what the impacts were.
We don't pay attention afterwards to how that was resolved in terms of someone was prosecuted, someone went to jail because of the action they took. And there's one area that do want to make a point, I don't think we have done so well, yet, at highlighting for organizations across the board, particularly those smaller in size that don't have a lot of resources.
Hospitals have become a big target because they have limited means to protect themselves. I think we really need to focus on understanding better through analysis. What the intrusion mechanisms are that enable the ransom ware attack to happen and help organizations understand what they can be doing better in terms of narrowing the term that gets used the attack surface, narrowing that opportunity. I think it's a two pronged approach.
We do a really good job of highlighting ransom ware as the problem. We don't do nearly as well a job of saying this is how ransom ware intrusions based on analysis that is happening and here is some things that you can do to narrow the risk profile of your organization.
(UNKNOWN): Let's follow up on that. My time has expired again thank you all for being here and I think you're right. It was hospitals maybe among institutions that were most vulnerable initially smaller hospitals that didn't have a more supplicated system.
My understanding is now moving to larger hospitals and other entities that have an even bigger impact on our critical infrastructure. Thank you Mr. Chairman. And maybe we'll follow up, Mr. Farmer, if that's okay with some follow up questions.
JOHNSON: Senator Ayotte?
AYOTTE: Thank you chairman. I would like to ask you Mr. Koppel based on the book that you wrote "Lights Out", what are the top three take a ways you want us to have today in terms of the action that we could take as a priority?
KOPPEL: Thank you Senator. Yes. I don't have has much familiarity with microphones as you do Mr. Chairman. Thank you for the question Senator. I think you're exactly right. We're focusing a little bit on the wrong issues.
And I think the key issue that we need to focus on, is even some of the most potentially successful measures that the industry is taking to defend itself. I think Mr. Aaronson will

concede, are still some time off in terms of the real affect of this.
The CRISP program that you referred to before, when Mr. Aaronson and I spoke about a year ago, I believe he told me that the goal was that by the end of 2015 that something like 0.4 percent of the industry would be covered.
And I'd like to give him an immediate opportunity to respond, maybe you're way ahead of that by now.
AARONSON: It is 0.4 percent of the number of electric utilities covering approximately 75 percent of all customers.
KOPPEL: OK. But it's still a minuscule percentage.
AARONSON: It's the right ones.
KOPPEL: OK. Except the right ones and the wrong ones are all connected.
AARONSON: So to that point, it's an important one, socializing the information. CRISP is wonderful for the companies that deploy it because they get near real time feedback about the impacts on their system.
Shortly after, that information goes to classified data bases is compared to those data bases and then is actually socialized through our electric infrastructure, I'm sorry EISAC, Electric Information Sharing and Analysis Center, to all of those 3,200 entities that you referenced. So the few that are deploying this technology are helping the whole.
KOPPEL: Except that the deployment of that information, in the age of the internet, we're talking about fractions of a second.
AYOTTE: With very quick development --
KOPPEL: With very quick development exactly is somewhat less than useful. My point is, I think we may be focusing on the wrong area at this moment. I think we have to conclude whether it is from EMP, whether it is from some space, weather incident or whether it is from the cyber attack, that the United States needs to begin preparing for the consequences of a successful cyber attack on the grid in particularly.
It was the grid indeed just does have such an impact on some of the other parts of the infrastructure. We don't have enough food. We are focused primarily on MRE's, meals ready to eat, which because they only have a lifespan, a shelf-span of five years, the government has not bought in sufficient quantity because it doesn't want to be sitting there with millions of MREs which are going to be no good after five years.
Even if we turn to freeze dried food, which I think is going to be the long-range answer, and if we were to begin today to try to accumulate the necessary amounts of freeze dried food, it would be two to three years if we started right now before we had an adequate supply.
We do not yet have adequate plans for evacuating if that indeed is what has to happen. Let's say a major city like New York is hit and a large part of the East Coast is without electric power. And some people, and we're talking about tens or hundreds of thousands of people, decide to evacuate, where are they going to go?
And I think it's a question that perhaps Gen. Dunbar can address, the degree to which each state is prepared to accept large numbers of internal refugees. I think we need to begin making plans. I think we need to begin communicating a state-to-state, federal government to state government and vice versa.
I know of at least one state on the East Coast whose preparations are that they would activate the National Guard. They would have their sheriff's department. They would have their state police standing there with maps, a bottle of water and a sandwich. And as refugees from nearby cities came through, they would give them the water, the food and the map, and show them where the nearest way out of town is.
AYOTTE: Wow.
KOPPEL: We assume because we're all Americans that every state is going to welcome vast numbers of internal refugees. I would suggest to this distinguished panel that is not necessarily

the case.
AYOTTE: Thank you, Mr. Koppel.
Mr. Aaronson, I wanted to follow up. And when I hear 24 percent of those that cover 75 percent of the infrastructure, I guess I have to agree with Mr. Koppel in terms of describing that as a very small if not minuscule amount.
But here's a question I have for you. Does -- what's your association's position on the installation of devices that would protect transformers that may be susceptible to damage from solar storms or EMP attacks?
AARONSON: So there is a lot of misinformation out there that there is a particular technology that would protect everything from everything. Earlier on we were discussing EMP. And there are very different natures of an electromagnetic pulse. You have a high- altitude nuclear weapon is one source...
AYOTTE: Well let me ask you this. Are you opposing installing...
AARONSON: No. Certainly not.
AYOTTE: ... devices to...
AARONSON: Certainly not. And in fact we are doing it though in a responsible way. Our real concern here is unintended consequences. One of the...
(CROSSTALK)
AYOTTE: What kind of unintended consequences?
AARONSON: Potential impact to the grid. When you put new widgets, whatever they may be, blockers, capacitors, resistors, on the grid, energy has to go someplace. And to Mr. Koppel's point I will agree completely that it is a balanced system. And new stuff can throw that balance...
AYOTTE: But here's our problem. So we're worried about new stuff. But we're facing a potential blackout situation that could cause mass chaos in our country.
So as we look at the risks we're facing versus deploying new technology, and obviously there are always new undertakings and new technology. Wouldn't you agree with me that this is a very important issue for industry to step up and address?
AARONSON: A hundred percent. And in fact we are.
There's a lot of money right now behind the Electric Power Research Institute, which is looking at just this. What would the threat be from the various kinds of EMP, whether it's a direct energy weapon, a nuclear weapon or a geomagnetic disturbance? And what are the appropriate mitigation strategies so that we do not have those unintended consequences?
We agree this is one of the risks. And we need to mitigate against it. But we don't want the solution to be worse than the -- worse than the threat...
AYOTTE: I'm not sure...
AARONSON: Especially...
AYOTTE: ... what could be worse than a blackout where we're handing people a sandwich and a bottle of water and giving them a map.
AARONSON: Well let's be clear with, especially -- let me break down each of the threats. If you're looking at geomagnetic disturbance, this is something that already happens all the time and that in fact we do have standards in place to deal with.
KOPPEL (?): Excuse me. Not at a massive level.
AARONNSON: We have...
KOPPEL (?): Let's be clear. Not at a massive level like the Carrington Effect.
AARONSON: The geomagnetic disturbance standard is ambivalent to whether it is a Carrington Event or just your typical solar max that we get every 11 years. It is operational procedures to protect the grid in the event of a coronal mass ejection.
If you then look at direct energy weapons, these are things that are mostly localized in impact, not all that different from throwing a Molotov cocktail or a bomb into a substation. It is bad,

but with 45,000 substations, we have a significant amount of redundancy.
The last one, looking at a high-altitude nuclear weapon, this is absolutely something that could happen. But I would posit it is a high-impact, but exceedingly low-probability event. This is not happening tomorrow.
So let's do the right thing to ensure that as we work to mitigate against this and many other threats that we're doing so in a risk- based and responsible way.
AYOTTE: With all respect, I think that government has a really important issue on the -- role when it comes to thinking about a nuclear attack. But let's just be clear. I serve on the Armed Services Committee. And we have Iran testing ballistic missiles right now. We have North Korea testing ballistic missiles. So we have a role in this.
I get it in terms of this. But what concerns me is that they're -- that's not the only source for potential EMP attack in terms of what could have an impact on this grid. And so what I would like to see is making sure that industry steps up.
My time is up. But I have a follow-up question. So perhaps I'll wait.
JOHNSON: Because I want a quick follow-up. How do you explain eight years after the 2008 EMP Commission the GAO reports to this committee we've done none of these -- performed any of these recommendations? So is GAO just wrong, or?
AARONSON (?): No, chairman. I appreciate you actually running through the litany of the 2008 report and sort of took notes as you were doing it. My understanding is the GAO report was looking at some of the things that government may or may not have -- may or may not have been doing over the course of the last eight years.
I can say, and this goes to Senator Ayotte as well, with respect to understanding the threat and what it might do to the grids, understanding the mitigation and the appropriate way to protect should an event like that happen, the industry is well underway in not just investigating but in some cases investing in mitigation. As companies build new control centers, as companies are building new substations and new control housing they are doing things to shield against EMP.
I note that we talked about restoration and replacement of equipment. That is something the Spare Transformer Equipment Program started in 2006 but has evolved dramatically with an eye toward any number of existential threats, whether it is combined cyber-physical attacks, really, really big storms, solar flares or even EMP, going down the line, looking at critical interdependencies. There is a lot of work happening in this space that mirrors the recommendations of the EMP Commission's report.
JOHNSON: OK. And again I'll reiterate my request to get that information on those replacement transformers.
Senator Heitkamp?
HEITKAMP: Kelly can finish.
AYOTTE: Thanks. I just have a follow-up question.
As I understand it DOD has developed some technologies that the utilities could actually use, hardware devices to protect electricity generators and pipeline compressor motors from certain cyber attacks. And I wanted to ask you, has the industry installed those hardware devices using some of the developments from the Department of Defense? And if not, why not?
AARONSON (?): So I'm not familiar with the specific devices that you're referring to. But I will say this. An enormous part of what the Sector Coordinating Council that I'm privileged to serve as part of the secretariat for is looking at is technology transfer from the government to the industry.
I will also say as a Congress you pointed out in your question before that this is something that government can help with as well. The Department of Defense in particular has had to contemplate how they would prosecute a nuclear war and had some really interesting information about what the impact of perhaps a nuclear weapon might look like to the grid.

The more we can do to get that information into the hands of the folks that are doing this research to apply it to the grid would be invaluable.
AYOTTE: So I'm going to submit for the record a follow-up question because as I understand you have the information and you have the ability to do this. And so I'll ask a very specific question and follow up for the record on this to get a more specific answer from you.
And I would like to thank all of our witnesses for being here, and the chairman.
Thank you, Senator Heitkamp. I really appreciate it.
JOHNSON: Thank you, Sen. Ayotte.
Sen. Heitkamp?
HEITKAMP: Thank you, Mr. Chairman.
Mr. Aaronson, a miracle happens every day. We walk over to the light switch and we turn it on and the lights come on. That's a pretty remarkable thing. And it's been a huge reason why this country has developed the way it has. So we all see huge consequences when we don't have access to power.
I also -- we're talking a lot about high tech threats and challenges. I would tell you that as a veteran of the utility industry you should also worry about low tech. You know my guys would tell you that a 22 in the right place could do almost as much damage as anything we're talking about today.
And so with some knowledge we know that a lot of our substations are not protected. They're not securitized. I would add that to the list of things that we ought to be thinking about as we look at protecting the grid.
AARONSON: If I can react to that. And again in my opening statement I remarked that we do have standards in place.
Standards in and of themselves are not security. If you mandate a 10-foot fence around everything the adversary brings a 12-foot ladder. So you want to make them bring that ladder. But you don't want to pretend that just because you have that you are secure.
Another component to security is this idea of resilience and redundancy. As you know, and I've mentioned a few times and so has Mr. Koppel, 45,000 substations. These are by definition soft targets. They are in communities. They are in cities. They are in valleys. They are on mountains. They are in rural areas.
So to try to protect everything from everything is a fool's errand. What we need to do is continue to build that capacity to be responsive and redundant when things happen. And I'll give you one quick example.
AARONSON: You may be familiar with an attack that happened in Silicon Valley a couple of years back. One or more people, we still don't know, shot up a substation, rendering inoperable 17 of the 21 transformers there. It was a bad attack. But I will note that the lights didn't even blink in San Francisco or Palo Alto. So it shows the enormous resilience of this grid.
HEITKAMP: But a coordinated attack with somebody with a great deal of knowledge about how you create redundancy on the grid could create real problems...
AARONSON: We...
HEITKAMP: ... in its classic or traditional attack?
FARMER: We agree completely and you're point about low tech, you know, Takkins (ph) rays (ph) are the simplest system, it's likely -- it's a lot easier for the hunter who had a bad day to go take pot shots than it is for a well coordinated combined cyber physical attack.
There's sort of an adversarial curve. Those, I want to quote John Brennan, the Director of the CIA, "those who can do this damage, don't want to, and those who want to can't." Now what I will say, that axiom is not static. There are certainly adversaries that are going to get more sophisticated --
HEITKAMP: And we can't afford the exception that proves the rule, that's the point.

FARMER: And we have to stay more sophisticated. And that's exactly right.
HEITKAMP: I am concerned about what happens, Major Dunbar, in the event or a catastrophic power outage as it relates to first responders and the resiliency and redundancy for first responders to operate in a world where we don't have access to electricity.
And I'm wondering what, what planning you've done in the state of Wisconsin or other organizations? In North Dakota we have an emergency management plan that's reviewed periodically with the national guard.
It has proven to be an invaluable resource when we look at the major floods where we did experience power outages, or huge snow storms with ice that takes down power lines. What kind of system should we be looking at for first responders so that we can in fact keep the peace in an event of a catastrophic outage?
DUNBAR: Thank you Senator. Wisconsin like all states we also have an emergency management plan that we update periodically. We've had experience with power outage but not in the scale that we're talking about, you know, long term and widespread. It's one thing if a small part of the community has power outage and the fire department and the police department have systems that they have right now to allow them to go into these areas and have generators and things like that and operate.
The scale we're talking about, we don't have plans. We're trying to get our head around what that would look like, the very point my colleagues of the panel are making in terms of -- it's one thing to have power outage for a couple of hours. And I joke with my wife, you know, the power being out for a couple hours, it's almost romantic, right, light a candle. It's not going to be romantic after a month. It's going to be a bad day, a bad week, a bad month in America. And add to that if people start to leave their homes. Big concern of mine, as Homeland Security Advisor in the state, if this happens in Milwaukee our largest city in Wisconsin or God forbid Chicago to our south and people start to leave their homes --
HEITKAMP: I just think it's something that we need to have that communications network. We need to have the ability to continue to manage an emergency response network, in the event of a catastrophic power outage. And, you know, so, prevention hugely important but also analyzing what we do with consequences. Mr. Koppel you mentioned food security. The world food program tests food all the time.
They have packets that they deliver or drop from the sky, they're just now transitioning to a high protein, high calorie product. Have you looked at all at what the world food program does to basically look at logistics in very difficult places and what they do with food security?
KOPPEL: No, I ma'am. I have not. But I would point out to the Senator, we're not talking about delivery. I think if there's one thing that the United States absolutely surpasses any other country in the world at it is delivery. I'm talking about availability. In a state like New York for example, you have 17 million people in the state. They have, let's say, 20 or 30 million MRE's stored in New York State. Do the math. You're talking about two days worth of food.
HEITKAMP: You might be a little concerned about delivery if the power goes out and you can't pump the gas.
KOPPEL: No, no, no you're --
HEITKAMP: I think you have to imagine as Hollywood does all the time, what an event like this looks like and what's the key components.
KOPPEL: You're absolutely right Senator and the other point I would make which I was discussing with General Dunbar before this session, is that we have a diminished number of military in uniform. And the fact of the matter is, if and when an event like this occurs, ultimately every state and the Federal government is going to be dependent upon the northern command, NORTHCOM (ph), we don't have enough troops to do what would be necessary in this kind of an event.
And if I may, one of your colleagues, Senator Ayotte, asked if there's anything we're leaving

out. I don't want this to be left out. The question of attribution, any other kind of attack that is launched against the United States, it's easy for our intelligence branches to discover instantaneously who did it, where the attack is coming from.
In the event of a cyber attack, attribution becomes one of the biggest problems. You can't respond if you don't know who did it. And it might take months before we actually determine, with any sense of certainty that would permit the President to respond who did it. That's a huge issue and one that needs to be examined more closely.
HEITKAMP: Well I think this is a great opportunity for us to have this conversation, to think about preparation because 90 percent of making this work is actually being prepared and being able to imagine the what if. And the what if's aren't related, always just to high falutin security attacks. There's some amazing things that can happen just conventionally with some very determined and bad people.
And so, General thank you so much for your service. We need to continue to recruit into our National Guard, that's a challenge for all of the National Guard today and talking about these issues publicly in terms of what importance it is for people to serve in uniform especially in the National Guard.
Mr. Koppel, your book is a perfect example and a great recruiting tool to tell people what in fact the value of that service is. So thank you much. Thank you Mr. Chairman.
JOHNSON: Thank you Senator Heitkamp. I just wanted to underscore where you said Mr. Koppel about availability. I come from a manufacturing background and I'm not exactly when the concept was developed but it's been decades. Just in time, that's how we run our economy, just in time so we do not have the availability. Senator Carper?
CARPER: Thank you Mr. Chairman. Mr. Koppel, you mentioned the number of people we have in uniform. I wore a uniform for about five years active and another 18 reserve, so I'm mindful for what you're saying. I also was commander in (ph) chief for eight years with Delaware National Guard as Governor of Delaware.
My last state of the state address that I gave, came off pretty well and finished up and we were having a reception later in Legislative Hall and a woman came up to me and she said "were you the governor when we had the blizzard of the century?" and I said yes ma'am. She said "were you the governor when we had the ice storm of the century?", I said yes ma'am.
You were the governor when we had the drought of the century, I said yes ma'am. And she said "were you the governor when we had the flood of the century?" and I said yes ma'am. And she said, you know what I think, I said no ma'am. I think you're bad luck.
Well fortunately the good luck is we had a great national guard. Frank Davila (ph), whom I know -- the General here knows as well, is our adjutant general in there, and whenever there is a blizzard, or an ice storm, or a flood or they don't do so much on droughts, but we have northeasters, we have hurricanes on the east coast and the national guard is always there.
Air guard, Army guard, and we are grateful for all that they do. Heidi -- Senator Heitkamp just said in her comments, I think that she mentioned that when you go pump gas in some kind of emergency, how electricity you can't pump gas and what that sort of leads to.
And what it leads me to is to say, you know, a lot of businesses, and a number of homes have diesel powered generators and they're there to provide electricity either for -- maybe for a home or for a compound or for a business. They are, they work, they also pollute a lot and at a time when we're trying to reduce a carbon emissions, they actually don't help out on that front.
I mentioned, in my opening statement, that there's some, I guess, 21st century tools, methods to meet those needs that are now met by diesel generators across the country.
And one of them was actually created at the old Moffett Field Naval Air Station where AVP3 squadrons (ph) were on the east -- on the west coast and with joint facility with NASA. I ask you for ideas on other, other similar technologies that we may be aware of that can help us when the electricity goes out.

And businesses need to be run, gas needs to be pumped, it could be a data center or a telecommunications company could be banking, it could be retail, be logistics, any number of things that depend on electricity. And when the power goes out they're not able in many cases to deliver, do their job and the rest of us are in a bind.
The technology that came out of the joint efforts at the old NASA base near Mountain View, California, ran into a company called Bloom Energy and they use fuel cells and hydrogen in order to create electricity for fairly small boxes. They call them Bloom boxes.
And actually rather large ones that could meet greater needs and they're installed across the country. Actually the Department of Navy uses them to some extent and I think other military -- units of our military are interested in exploring those capabilities.
I think a couple of state, we manufacture some of those Bloom boxes in Delaware. I think New Hampshire, Ohio now use fuel cells like these but they also contribute heavily to manufacturing of fuel cells. But my question for our witnesses is how, at all, how can we change our policies and practices to further rely on innovated solutions like fuel cells to increase the security and resilience of our critical infrastructure?
DUNBAR: This is one thing that's being done. And go ahead please Mr. Koppel.
KOPPEL: If I may Senator, two points. One, I have a generator at home that runs on natural gas, problem is the natural gas has to get pumped to my home. And the pump operates on the basis of electricity. So if we have a massive grid failure, I guess that natural gas isn't going to make it to my house either.
The other point is I interviewed a retired lieutenant general from the Air Force who indeed is engaged in exactly the kind of work you're talking about. He and his partners have noted that the nuclear generators that fuel a number of our Navy ships have now had 50 years of successful operation without a single accident.
The theory is if we could create a number of these nuclear power generators and put them on military bases around the country, they could not only serve those military bases but there would be additional power to run critical infrastructure in neighboring communities.
I asked the general if the president gave him the go ahead tomorrow to develop that capability how long would it take. His answer, 10 years.
CARPER: My -- both my boys are Boy Scouts. I used to take our Scout troop, Troop 67 from Wilmington, Del. to the Norfolk Naval Station a couple -- maybe three or four years. Spend the weekend, sleep in the Brigs, eat in the Galley and criss (ph) climb all over ships, submarines, aircraft carriers.
And one Sunday we went to (inaudible) and we went to Teddy Roosevelt. We go to tour the Teddy Roosevelt. And we had about 25, 30 Scouts, maybe a half dozen adult supervisors. Anyway, we get to the bridge of the ship and we're met by the commanding officer of the ship. He's a captain, Navy captain. And he said to our group, he said, "Boys, when the Teddy Roosevelt goes to sea it's 1,000 feet long." And the boys went "ooh."
And he said, "Boys, when the Teddy Roosevelt goes to sea it has 5,000 sailors on board." And the boys went "ooh."
He said, "Boys, when the Teddy Roosevelt goes to sea it has 75 aircraft on board." And the boys went "ooh."
And then he said, "Boys, when the Teddy Roosevelt goes to sea, it refuels once every 25 years." And the adults went "ooh."
And we had -- the hearing we just had, the mark-up we just had I was late for is I'm senior Democrat on the committee called Nuclear Safety. We had our Nuclear Safety -- and we're actually focused on just this thing, new generation nuclear power, modular, small modular. And actually with the technology where you can use spent fuel rods from other nuclear power plants anti-derive electricity from them, and so there's -- so really exciting stuff going on. Maybe a lot smaller, easier to build, maintain and so forth, so, and redundant with more

resiliency.
So thank you for that idea. Any other ideas, please?
AARONSON: Yes, Senator Carper. I appreciate some of the things that Mr. Koppel said. I want to underscore one. He talked about how his generator relies on natural gas, but the natural gas relies on electricity. I'd go even further back to the electricity relies on natural gas. So there are profound interdependencies throughout. And I think that's something that this sector, which has always been held up as the most critical, really gets just as a matter of course and is working across those critically interdependent sectors.
With respect to technology as a solution to this, I would say yes, technology, things like the bloom boxes and other distributed resources come with some added resilience and redundancy. They also come with -- it's a double edged sword. They also come with the phrase that's been used and added, attack surface.
If you look -- I'm from New Jersey originally. If you look at what happened during Super Storm Sandy, several hundred circuits were destroyed and had to be fixed, and took between 10 days and two weeks to get the power back on. Had there been distributed resources, maybe 30 million from all over the Greater New York Metropolitan Area, we'd probably still be restoring.
So I don't want to pretend that those devices in and of themselves equal security or redundancy. They are a component. They are a tool in the toolbox.
The last thing I'd say is with respect to military installations and that sort of a partnership. Yes, in fact siting generation on military installations for their use and then for the community's use in the event of an incident is something that is happening and certainly could be happening more.
So I think that there are a lot of interesting ways -- I want to be very careful to say we're open to anything. I think anything that enhances the resilience and redundancy of the service we provide is something we all ought to be exploring. And it is the value of the Sector Coordinating Council and the CEO and senior government leadership, which are setting that strategic course.
As opposed to finding these little tactical things that we could be doing, let's learn from some of those experiences like Ukraine, like Metcalf, like Sandy and Katrina, like the wildfires in California and like our experience putting things on military installations. And let's build on those. And figure out -- let's have an automated response to some of these incidents. And let's have a capacity to go back to the 1960s and be able to support civilization without automation.
CARPER: All right. Thank you.
My time is expired, but Mr. Koppel, go ahead.
KOPPEL: If I could just add one footnote to what Mr. Aaronson just said.
Prior to the deregulation of the power industry, military bases in this country generated their own power. And the Pentagon came under great pressure from this particular geographic location on Capitol Hill to save money by using private industry to generate the power on the bases. So to a certain extent we're talking about going back to the future.
JOHNSON: All right. Go ahead.
CARPER: Quick side note, Mr. Chairman.
Sandy was about three or four years ago, but actually there were balloon boxes that were -- that deployed previously before Sandy hit. And they were actually used I think to go to effect. So that's I think some encouraging news.
Thank you so much for being here. It's a great hearing. Thanks so much.
JOHNSON: Thank you, Senator Carper.
What I'm going to do is kind of go down the line there and give everybody a chance to make a final comment. But I do want to quick explore what I am assuming is the major -- the primary weak link. And I think it really is transmission. First of all, is that correct?

I mean we can -- yes. You can shut down a power station. But there will be other power stations that might survive. But it's really -- let's say you do these things on military bases. And you can maybe distribute within the military base but then going further and further out. Transmission is really sort of the weak link here isn't it?
AARONSON (?): I mean I'll quibble with the word. I wouldn't call it a weak link. It is actually exceedingly secure because it's so redundant. But it is I think the primary focus of our attention for security.
JOHNSON: But again, depending on maybe a very low probability of an EMP or a massive GMD, the weak links in that transmission system are these large power transformers, correct?
AARONSON (?): They are the lifeblood of the transmission system.
JOHNSON: OK. What determines the 200 to 700 critical transformers? Is that size? Is it location? Why are they critical versus the tens of thousands of other ones that Mr. Koppel was talking about?
AARONSON (?): So yes. It is size. It is what they serve. There's any number of criteria that each individual company would know as to why a particular transformer is critical.
And I'll just tell a quick anecdote. There's a company that had identified several of their transformers to be critical and disclosed them as so. And then that list changed and somebody asked why. And the answer was they built another substation.
So there are certain substations that are taking load in very critical areas -- or I'm sorry, taking electricity in very critical areas and transmitting it. And so as a result those are your priority transformers.
And let's put it this way. If you have 45,000 priorities you have none. So we really do have to hone in on those that are the most critical to the system.
JOHNSON: So would you agree with me that -- my concern has always been these large power transformers. That is -- those are the things we must protect, we must have redundancy for. There're other concerns.
But that is -- again, I'm coming from a manufacturing background. What's the root cause? Is that sort of the most critical thing that we should be turning our attention to?
AARONSON (?): There are...
(CROSSTALK)
JOHNSON: (Inaudible) those?
AARONSON (?): There are a lot of critical things that we need to be doing. But I think I do agree with your statement. And the industry agrees with your statement, which is why we have developed so much excess capacity, and again, working with folks like Mr. Farmer and the railroads, the ability to move these things around.
You know I've heard too often this notion of if there were something really bad that happens we would "reengineer the system". That's a hard thing for a non-engineer to fully appreciate. So what we are starting to do -- and I shouldn't say starting. What we have been doing in the recent -- recently is to explore what does reengineer the system mean and plan for that so we can do it more effectively and efficiently if and when something does happen.
JOHNSON: OK.
Let me start with you, General Dunbar. Closing comments?
DUNBAR: Well, senator, thank you for the opportunity to be with you. I would foot stop I think four things at the end here.
One, just to reiterate, the importance from my mind of trying to do what's possible from my level at a state level. A lot of the things you're talking about are beyond my level. If something happens long term it's my intent to try and keep citizens in their homes. And that means making sure we've got water and sewage systems so that they're not desiring to leave the city. Big problem if that happens.
If there's a long-term power outage, the industry talks about things like islanding and

microgriding. I think there is great value in trying to think through how we do that as a country if we have to do that after an event.
The third thing I'll mention, and again I'm not an expert. But it's my understanding that our black start capability used to be largely based on coal. We're moving as a country away from coal for the reasons that we're doing it.
I'm not making a political statement. From a public safety point of view, if we have issue with generating and transmitting natural gas and coal will allow a better black start, we ought to reserve some of that black start capability from a public safety point of view.
And the last thing I'll mention is the information sharing piece. The federal government's doing a lot of great work with utilities and with industry. Often the states aren't part of that information sharing. I think we have a role to play and we should be part of that information sharing.
Thank you.
JOHNSON: Thank you, general.
Mr. Farmer?
FARMER: Thank you, sir, very much for the opportunity. Thank you, Senator Carper as well.
I'll open by referencing a point you asked about technology development. And really the key to advancing technological solutions is a combination of innovation and investment. And to the point about coordination, what the Cross-Sector Council as (inaudible) for Cross- Sector Council.
And you can hear the term council and coordinated committee and think these just seem to be another range of inside the beltway groups. But they're not.
And particularly his Cross-Sector Council I'm privileged to represent dates back 16 years now. That's a commitment by industry to work in concert across sectors and with government to matters related to critical infrastructure protection.
And there's a laboratory of ideas there. There's an ability to bring all that talent, that expertise together in industry and government to look at the sorts of problems we talked about today. And in some case we can look to near-term solutions that can help ameliorate some of the concerns. And then look to a technological development program for those longer-term innovative investments.
DHS is starting this year and coordinated with our council and its development a resilience challenge program. The purpose of that is to do exactly what Senator Carper alluded to. Let's inspire some innovative ideas on how we can address some of these challenges.
And again, you're looking at a two-phased approach. In some cases there are things we can do to mitigate problems now. And some are going to take a long time.
But just because it takes a long time doesn't mean we should be innovating and investing in that direction. Quite the contrary, if it's going to take a long time let's get moving on it. Let's use initiatives like a resilience challenge or some other similar investment program where we can combine public and private funds to advance these efforts.
FARMER: You know this -- as I said, this council's been in effect for 16 years. It's a tremendous forum to create a foundation for the sort of cooperation between industry and government that can make progress in these important areas.
Think about this term public-private partnership. This is a new way of government and industry working together, sharing experiences, expertise, information, ideas on a common goal. What can we do together to take the sorts of actions, near term and long term, to enhance how well our infrastructure's protected and how well it can withstand various types of threats? And we're taking innovations in this process that would have seemed inconceivable just a few years ago.
The day of the Paris attacks we ratified an information sharing approach that was exercised just a few days earlier that we had to put into effect within a matter of hours. We've built on

that since then.
And to the general's point about integrating state and local government, we said to DHS there're going to be occasions when whether it's a cyber threat or a physical threat or some broader concern about electromagnetic pulse, as one example, where you're going to want to share very quickly classified information. And you can't wait days or weeks to get people into Washington, D.C. to do that.
You got this tremendous infrastructure in the fusion centers that allow us to get on a secure video teleconference. Why aren't we using it to good effect to ensure that what formerly might've taken days or weeks can now be accomplished in a matter of hours?
On April 26 of this year we exercised that capability. The participants didn't have notice of precisely when this event was going to occur. They received an emergency notification that morning. It simply said go to the fusion center where your clearance has been validated for a classified presentation by DHS.
And we exercised it in six cities simultaneously and it worked. And we're going to exercise it again before our councils come together, federal government, industry, state and local for a meeting in early July.
The point is the coordination that this process allows creates opportunities for a kind of interaction between government and industry that simply has not happened at this level before. And that's the strength of the perspective that I think this cross-sector group brings.
Some of these challenges are very daunting. Some of them are so daunting that inertia can set in. You kind of throw up your hands and say what to do about it. But that's precisely what this group is designed to avoid. It's designed to bring together the right subject matter expertise, and through representatives like Scott and I to reach back for more.
So I thank you for the chance to talk about what we do.
JOHNSON: I appreciate that. And you know you can have the most wonderful processes. But one of the things I noticed about Washington, D.C., there's an affliction that affects this place. And it's called the denial of reality. And I think we're -- in many respects I think a lot of the discussion here is centered on the fact that we just deny this reality. The possibility of the low probability event could be just catastrophic.
Mr. Koppel, I appreciate the way you opened your book with the little scenario that if people don't read the entire book at least read that. OK. You'll lay out what a potential reality would look like if we lose power for more than six hours. It starts filtering into even days and then weeks and then months.
So the first thing we have to do is recognize and admit this possibility, the reality and start -- because otherwise we will never take the first step and these processes take a very long time. But, Mr. Koppel?
KOPPEL: I thank you, Mr. Chairman, Mr. Ranking Member.
I think the observation I want to make most of all is that the Chinese are already in our power grid. The Russians are already inside our power grid. They may lack the motivation because of the interrelationship that we have with both those governments to take action against our grid. But they can do it.
We live in an age of cyber warfare. Cyber warfare is going on all the time on every different stage of our lives.
The fact that the governments like North Korea, for example, which are desperately seeking the same kind of cyber sophistication that the Russians and the Chinese have, the fact that they don't yet have it shouldn't be the source of any particular comfort to us. The fact that organizations like ISIS, which still probably have $1 billion to $2 billion in resources, have not yet used that money to buy the expertise to attempt perhaps a cruder kind of cyber attack on our power grid shouldn't give us a great deal of confidence.
And I would like to add one other point that I suspect will be politically very controversial. I

don't think the Department of Homeland Security is best equipped to deal with this issue. The National Security Agency is by far the most sophisticated body in the U.S. government to deal with it.
And I think leaving it up to a department that has one of the lowest rankings in federal government, and allowing ourselves to be concerned more about privacy than about security clearly is the subject for a whole other hearing. But I didn't want to let this one conclude without at least raising the issue.
Thank you, Mr. Chairman.
JOHNSON: I appreciate your comments. And again, I appreciate your book.
Mr. Aaronson?
AARONSON: Chairman Johnson, Senator Carper, it may surprise you to hear thank you. I appreciate you all holding this hearing. And it also may surprise you, the industry agrees with a lot of what is being said.
We do take this seriously. And we do understand the threats that exist out there. I'll tell you a quick anecdote.
About three years ago, four years ago now, several CEOs were in Colorado Springs for a board meeting, about 70 of them. We brought them over to NORTHCOM for a classified briefing. And the CEOs heard from the intelligence community, from the Department of Defense, from other agencies some of the threats that were out there.
And what came as a surprise I think to the government participants was the CEOs weren't raising their hands saying is there really a problem, we don't see this. Yes, there is a problem. What can we do about it? And from that one meeting has born this incredibly effective relationship between CEOs and senior government officials.
Now I occasionally joke that CEOs don't do work. But they do provide accountability. They do provide a direction. They do provide resources. And when the people in the corner office care about something it is amazing how the rest of the enterprise does.
So what we are seeing is up to and including the CEO levels, security of the electric grid is a priority for this industry. In Mr. Koppel's book there is a chapter titled Guardians of the Grid. We are. And we take that very, very seriously.
The other thing I'd leave you with is there are a lot of movie script scenarios that they've been referred to. I had the opportunity to testify in a state capital and had to tell whether or not Die Hard 4 was actually a plausible scenario. Let's not use movie scripts to dictate public policy. My problem is when I come into venues like this I am giving issues of popular mechanics and resilience and redundancy and all the things that can and might happen might not happen and we're studying it. I get bored just saying that.
So I understand that we need to be informing public policy in a reasonable and rational way, understanding that these high-impact/low- probability events are something we absolutely have to put on the spectrum. But also understanding that there are a lot of things that happen day-to-day that require our attention as well. It's where those -- the Chinese, other sophisticated adversaries, that is where government and industry absolutely have to partner.
Now I don't have an opinion on what Mr. Koppel said about whether or not DHS is the right place or the wrong place. We have had a wonderful experience working with the Department of Homeland Security and particularly NPPD.
But I would suggest this is a whole of community issue. And by whole of community I do mean north-south between the government and the industry, the industry and the government, and east-west across the critical sectors. And Tom talked about what we're doing with the railroads. But we are seeing very similar partnerships with communications, with financial services, with the water sector, with the gas sector.
So we are learning. We are looking at preparation. You know you build the roof when it isn't raining. And that is what we are doing today. I think the industry has learned great -- has

learned some great lessons from what's happened in Ukraine, from what's happened from the quite literally decades of natural disasters.
And I want to leave you with the one parting thought that while there are 45,000 substations in the United States, it is the definition of a soft target. It is also exceedingly resilient and redundant. There's a lot of excess capacity. And we're working to develop that. We're working to grow that continually.
And then the last thing I would say is as you all consider policies, let's not have a rush toward automation. Let's not have a rush toward the newest, shiniest object. Let's think about how policy decisions just as we think about how investment decisions are -- will have an impact on the security reliability and the resilience of the grid.
So again, I thank you for having me here today.
JOHNSON: I'm the guy that's talking about manual breakers in Ukraine that kind of saved him.
Senator Carper?
CARPER: Thanks. I just wanted to come back to the question of the competency of the Department of Homeland Security.
Mr. Koppel, I shared your views four or five, six years ago. Senator, a previous chair of this committee, Susan Collins, Joe Lieberman and me, and now Senator Johnson have worked long and hard to try to change that reality. And that was the reality for a half dozen years, even before three or four years ago.
And we have -- I won't go through the entire list of things. But there was a time -- we used to have a problem when I was governor of Delaware. We'd hire people to work in information technology, hire them, train them, put them to work. Somebody would come along and hire them away.
And (inaudible). You know what I mean. Hire some more people and they'd go to work in IT. And somebody would hire them away.
Well as it turns out, National Security Agency has the ability to hire people, pay them more money, retention bonuses, that sort of thing. Department of Homeland Security never had that. So they hired people, trained them and they'd get hired away by NSA.
And one of the things we've done is to make sure that Homeland Security has the ability to actually compete. And the market's really tough in terms of hiring -- between hiring and retaining cyber warriors.
I won't go through all the other things that we've done. But we have worked long and hard for a few years. And what is the old saying, the old tagline under the Oldsmobiles? This is not your grandfather's Oldsmobile.
This is not the Department of Homeland Security of even four or five years ago. And that -- can they do better? Sure they can do better. They can always do better.
The last thing I would say, the general here is wearing Air Force uniform. I used to wear a Navy uniform. And there's a friendly inter-service rivalry, as you know. And I was with an Army guy the other day. And he was jagging me about being in the Navy. And I said you know we wear different uniforms, but we're on the same team.
We're on the same team. And the same is true with Homeland Security and NSA. And we need both of them to be really playing -- bringing their A game to the contest every day because as you suggest, there's a real battle across the land.
The other thing I'd say is I was in China about a month ago and you may recall President Xi -- Chinese President Xi was here in last September. One of the things that our president confronted him about was cyber theft for stealing intellectual property for economic advantage. Basically said to him you got to stop this. The Chinese guy said oh, we don't do that. Well they do. They have done it for years.
But you know what happened? The president said -- our president said in so many words, you

keep doing this and the kind of sanctions we've imposed on Iran, we can do that with you. And we're your major trading partner. So think about that.
Since then the incidents of cyber theft for intellectual property for economic advantage with respect to China has gone down, down, down. It's pretty interesting. A guy named Dave DeWalt who runs FireEye, FireEye, Mandiant was big cybersecurity company, have reported just last week, two weeks ago. Said we'd seen a continued drop there.
And the other thing, Iran for many years was going after our banks trying to shut down our banks, going on their websites, close them down. And it's called distributed denial of service. And one week after we entered into this joint agreement with Iran and five other nations those attacks stopped, they just stopped.
And so just keep that in mind is, there's things we can do and we need to do to be resilient. But chairman, I believe very much in root causes. And sometimes -- now China had some intellectual property they want to protect they have a dog in the fight. And they also have the threat if they keep up this stuff they'll pay a price for that.
The Iranians, they're given a chance to be a good player. We'll see if they continue to keep their word. I think so far they have. And at least those attacks on our financial institutions have stopped.
JOHNSON: Thanks, Senator Carper.
Let me just close out the hearing reminding everybody what Dr. Richard Garwin, again who Enrico Fermi referred to as one of the few true geniuses he ever met, in testimony before this committee remind us that a solar event on the order of -- order of magnitude of the Carrington Effect happens once about every 100 years.
In other words, we talked about low-probability high catastrophic. That's about a 10 percent chance every decade, every 10 years of having a massive solar storm affect our electrical grid. So, maybe not so low probability.
But again, I want to thank all the witnesses. I think this has been an extremely good hearing. It certainly helped lay out a reality that hopefully we stop denying.
This hearing record will remain open for 15 days until June 2 at 5:00 p.m. for the submission of statements for the record and questions for the record. This hearing is adjourned.
END
May 18, 2016 18:41 ET .EOF