Commission on Enhancing National Cybersecurity

Established by Executive Order 13718,
Commission on Enhancing National Cybersecurity

University of Houston
Hilton University of Houston
Conrad Room – 2nd Floor
4450 University Drive, Houston, TX

MEETING MINUTES

The Commission on Enhancing National Cybersecurity (Commission) was convened for its fourth public meeting at 9:05 a.m., Central Time on July 14, 2016 at the University of Houston, Houston, Texas. The meeting in its entirety was open to the public. For a list of meeting participants, please see Annex A.

Welcome and Overview

Dr. Paula Myrick Short, Senior Vice Chancellor for Academic Affairs, University of Houston System; Senior Vice President for Academic Affairs and Provost, University of Houston

Dr. Paula Myrick Short welcomed the Commission. Dr. Short is the Vice Chancellor of Academic Affairs for the University of Houston System, and Senior Vice President for Academic Affairs and Provost at the University of Houston main campus. Dr. Short introduced Kiersten Todt, Executive Director for the Commission.

Kiersten Todt, Executive Director, Commission on Enhancing National Cybersecurity

I'd like to thank Dr. Short, the University of Houston, and Hilton Hotels for hosting the event. I would also thank Jason Smith, Vice President for Governmental Affairs for the University of Houston, and Sarah Damato and Linda Hall from the University of Houston Hilton. She opened the meeting and turned it over to Samuel J. Palmisano (Vice Chair). Today's meeting represents the third of five public meetings.

Meeting Opening and Remarks

Samuel J. Palmisano, Commission Vice-Chair

I would like to thank everyone from the university, and the Hilton for welcoming us today. President Obama has asked the Commission to examine cybersecurity and critical infrastructure to ensure that we have a secure, resilient, and protected internet in order to protect commercial activity and society as a whole. We need to examine what can be done to ensure the critical infrastructure of the government. We have received a great amount of good input from our previous public sessions and look forward to the session today.

Panel 1 Current and Future Effect of Critical Infrastructure on the Digital Economy.

Robert “Bob” Kolasky, Deputy Assistant Secretary, Office of Infrastructure Protection, U.S. Department of Homeland Security

Steve Mustard, Cybersecurity Committee Chair, Automation Federation

Dr. Subhash Paluru, Senior VP & Sierra Nevada Regional Manager, Western Area Power Administration

Mark Webster, Assistant Special Agent in Charge, FBI-Houston Division

Marty Edwards, Director, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), a division of the National Cybersecurity and Communications Integration Center (NCCIC) in the Department of Homeland Security (DHS)

If we look at society's cyber-enabled systems, they're not only our smart phones, or the computers on our desks, there is a category of computers that is largely unspoken of. They run silently in the background. I'm speaking of industrial control systems, and Supervisory Control and Data Acquisition (SCADA) systems: small embedded processors and computers that are essentially all around us in critical infrastructures such as the electrical grid, the elevators in this hotel, the heating, HVAC systems. Originally, these systems were designed to be completely isolated from other systems, and ran that way, often for decades at a time.

Over the years, however, we designed these systems to interconnected those systems for business efficiencies, such as corporate IT environments and the internet. Once we start down the path of connecting everything to everything, we have to consider cybersecurity risk factors that arise. We haven't done as good a job as we should have.

Those systems were never intended to be connected in the way they are now. Some have suggested designing "old fashioned" analog or manual safeguards in order to protect systems from their digital environment. It's been characterized as the "dumbing down" things like the smart grid. It should be viewed more a prudent engineering practice, to examine what manual safeguards and overrides should be put into place to keep society safe and secure. ICS-CERT products and services have helped with some of this. We do private sector and all levels of government infrastructure assessments and provide recommendations to the asset owners to improve security.

Robert "Bob" Kolasky, Deputy Assistant Secretary, Office of Infrastructure Protection, U.S. Department of Homeland Security

The Office of Infrastructure Protection at DHS falls within the National Programs Directorate. It is the de-facto cybersecurity for DHS. Congress has proposed legislation rename the directorate to reflect this status. In that role, we are responsible for enhancing the nation's critical infrastructure against all hazards including cyber-threats. We also provide federal and network security. The DHS mission has evolved to include physical and cyber threats.

The nature of infrastructure operations in the digital economy has broadened and altered what can be considered critical infrastructure. The reality of infrastructure control has shifted the critical infrastructure landscape. Supply chains have expanded and become more interconnected. Space-based position and time systems have expanded as well. There are interdependencies across sectors and networks. They are key to the nation's security.

Issued in 2013 Presidential Policy Directive (PPD) 21 established policy for national critical infrastructure resilience. It defines sixteen critical infrastructure sectors, and defines the need for

an integrated cyber approach to risk management, the importance of public/private partnerships, expands the mandate for information sharing, raising critical infrastructure awareness, and calls for additional development efforts.

Two years after the task force disbanded, Mr. Kolasky believes the nation has been well-served by PPD21 and Executive Order (EO) 13636. There has also been a heightened awareness of cybersecurity across critical infrastructure. For example, the environment has been greatly enhanced by improvements in automated information-sharing. Based on recently-passed legislation, the National Cybersecurity and Communications Integration Center (NCCIC), serves as the hub for critical infrastructure information sharing by implementing automated information-sharing and identifying critical infrastructure threat indicators.

Additionally, (referring to an executive order signed in 2014), information sharing analysis organizations continue to develop to promote public/private and private/private information sharing. The Department of Energy has partnered with the intelligence community to build programs to share classified and unclassified critical infrastructure information.

Second, the National Institute of Standards and Technology (NIST) critical infrastructure framework has served as a common risk-management approach for critical infrastructure. For example, a great majority of the sixteen critical infrastructure sectors have published sector-specific implementation guidance on how best to integrate the framework within their respective sectors. The framework has been increasingly used as the basis for an expanding critical infrastructure insurance market, and regulating agencies are working to harmonize their regulatory approaches within the NIST framework.

Third, there is a heightened awareness of critical infrastructure as a business imperative. For example, the electric sector has elevated its coordinating counsel to a chief administrative officer level, focusing on cyber resilience. The nuclear sector is coordinating a joint exercise with the UK scheduled for November 2016.

DHS utilizes four lines of business to help the private sector enhance cyber management:

The first is person-to-person and machine-to-machine information-sharing through bulletins. There are private sector companies who sit on the NCCIC floor and participate in joint events to disseminate their findings.

The second is to disseminate and enhance best practices by advocating for adoption of the NIST framework through workshops and webinars, in order to help small and medium-sized businesses understand the framework. We also do risk assessments to enable businesses to better understand their current risks. The assessments are derived from questionnaires, and from penetration tests, one of which has been scheduled with the University of Houston. Finally, we have an initiative to educate boards of directors and other top-level managers to better understand and supervise implementation of the critical infrastructure framework within their respective organizations.

The third relates to incident response. DHS assists in identifying the point of penetration by an adversary as it affects their network and assists to kick the adversary off of the network. DHS is frequently onsite with representatives of law enforcement to identify and bring the adversary to justice, however, our focus is on the victim and how best to restore service as soon as possible.

The fourth is broader: to assist in shaping the entire cybersecurity ecosystem, including work to stimulate the insurance industry, encouraging agencies and businesses to incorporate critical infrastructure security into their software, and to increase the number of cybersecurity professionals in the workforce. The task force works closely with the other organizations such as the National Science Foundation (NSF), the National Security Agency (NSA), and NIST.

The fifth relates to Federal cybersecurity, but that takes on a more operational direction.

I would urge the commission to continue to consider the following ideas. The current approach to protecting critical infrastructure has raised many benefits, but there are still opportunities to raise security in the face of the current threat environment. As deliberations continue, I would offer these areas to consider:

- Improved assessment of cyber risk to inform regulatory decision-making, and understanding the cost of not investing in cybersecurity and to allow for tradeoff decisions;
- Enhanced risk management for cyber physical systems to work with the Internet of Things to enhance design and resilience
- Improved coordination between cybersecurity, DHS, and emergency management professionals to develop plans to minimize the effects of cybersecurity attacks.
- New solutions for government and industry to more flexibly work together to innovate in cases of emerging risk and to avoid possible roadblocks caused by governmental legislation.
- Implementing critical infrastructure strategies in environments constrained by limited resources common to small and medium-sized businesses.

We have the right tools in place for the government and private sector to work together. These tools only work with time and energy expended on the government side to make them worthwhile to industry, the ability to share multi-directional information, legal protections to enable collaboration, and most importantly trust to allow government and industry to collaborate to solve problems.

Steve Mustard, Cybersecurity Committee Chair, Automation Federation

The Automation Federation is a seventeen-member global umbrella 501-C3 (tax-exempt) organization for all entities engaged in automation-related activity. The federation enables its members to more effectively fulfill their missions, advance the science and engineering related to automation, and to develop the workforce to capitalize on that technology. The Federation is the "voice of automation."

Mr. Mustard is an expert in the field of automated industrial control systems. His presentation is based on his frequent visits to critical infrastructures around the world. The cybersecurity threat to the nation's critical infrastructure is significant. There must be immediate action to avoid potential catastrophic attacks which could result in loss of life, damage to the environment, and/or serious economic consequences.

It is often the case that critical infrastructure is controlled by antiquated technology where conventional critical infrastructure measures are difficult to apply. It could take months or even years to take these systems out of service. There remains a dearth of competent personnel to

address these issues and who appreciate the key differences between information and operational technology.

As a consequence, safeguards are limited to perimeter security without controlling access and backup/recovery systems. The greatest challenge to cybersecurity management is complacency and that historically, attacks have affected multiple systems simultaneously. Though security technology has improved, people-oriented threats have increased. Social engineering methods are the dominant attack vector. People continue to use bad practices. Most cybersecurity budgets are biased toward technology. Though there is vigilance in following physical safety practices, the same cannot be said regarding cybersecurity. People continue to ignore the dangers inherent in downloading attachments.

Technology is only a third of the cybersecurity challenge, the other parts being processes and people. Unfortunately, resources are weighted toward technological preparedness, and not on improving awareness and producing workable policies. The industrial sector already has a proven strategy to address physical security. The same idea must be applied to cybersecurity as well. While workers in an industrial environment are rightfully reprimanded for neglecting physical safety regulations, the level of control is not as stringent in preventing an employee from introducing un-scanned devices into computerized systems.

The industrial sector also has effective practices to manage change, but these are often not applied to industrial control systems. The result: changes are made without adequate testing, record-keeping is poorly organized, or even non-existent. Incident response plans too often lack provision for cybersecurity. An attack may be ignored because the physical effects may not be identified. The solution: a fundamental shakeup in the culture. There are existing resources to address cybersecurity:

IEC 62443 – Industrial Network and System Security – provides direction to enhance industrial network and system security. The cybersecurity framework provides a good starting point for organizing responses to cyber-attacks by comparing what entities *should* be doing, as opposed to what they currently *are* doing. The workforce should be enhanced to train and equip additional cybersecurity specialists, supplemented by certification-based programs. Products should be security-certified. However, none of these strategies should be reduced to ineffective checklists.

We recommend the following as constructive actions to address cybersecurity:

- A major change must be made to realistically present the threat to cybersecurity.
- Timely education and training should be implemented to address people of all ages, from children to employees.
- Cybersecurity skills should be part of the standard competency framework when hiring industrial employees. The U.S. Department of Labor automation competency model, and the cybersecurity industry model provide the structure to implement proactive strategies.
- Specialist industrial control systems cybersecurity training is required to bring stakeholders up to the necessary skill level.
- Products should be verified as compliant by competent third-party entities. Consumer demand will drive vendors to adopt these policies.

– If these measures are implemented across all sectors, the industry will have taken a major step to ensure cybersecurity.

Dr. Subhash Paluru, Senior Vice President and Sierra Nevada Regional Manager, Western Area Power Administration (WAPA).

Dr. Paluru has worked in the electrical industry for twenty years. WAPA is one of four power marketing agencies directed by the Department of Energy, and operates in fifteen states over 17,000 miles of transmission lines, with over 300 substations, over 200,000 structures, and over 1,000 communication centers to operate the grid.

He manages the division that controls transmission to Northern California and Nevada. The division manages California's central valley, the nation's breadbasket. WAPA receives signals at the rate of two per second regarding the state of physical and cyber components of the grid. Cybersecurity is as important in the substations as it is in the system itself. IT solutions for all fifteen states are managed at a central location. In order to protect the grid, communication is maintained with other utilities.

While technological solutions are important, the need to train employees to use the technology is even more important, especially since WAPA resources are not comparable to those deployed by the larger utilities. To implement changes, we visit each region to educate local employees to bolster the weakest links in the system.

Among the regulatory agencies supporting WAPA is the North American Energy Regulatory Cooperation (NAERC) which issues mandatory critical infrastructure requirements. WAPA had no issues raised by NAERC audits in the past few years. We are proud of that record, but we also recognize the critical role played by WAPA, since, without electricity, all other critical infrastructure systems cease to function.

Education is important, so that clients understand the linkage between the introduction of improved technology with the necessary rate increases to enable pull implementation. Timely information sharing is critical to better ascertain the nature of any threat to our critical infrastructure. It happened that one week after a potential threat, he received an email alerting him to the incident.

WAPA is currently piloting an information sharing effort for utilities in the western United States by meeting with the CEOs to establish a network in which to share secure email communications in the event of an incident.

Mark Webster, Assistant Special Agent in Charge in the FBI-Houston Division.

The FBI welcomes the commission's leadership in enhancing cybersecurity. The industry should implement the following: patches to software and firmware are properly tested and deployed; minimize access to privileged user accounts and only used when necessary; establish a baseline of application and security measures across networks in order to distinguish between malicious and benign activity; critical infrastructure systems should be isolated from non-critical systems; identify where critical information is stored and managed to prioritize network security; develop an efficient incidence response plan; increased cooperation between the federal government and

private industry and establishing a trusting relationship between the FBI and clients before an incident occurs.

Panel 1 Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Mr. Sullivan: "When does Pokémon Go become critical infrastructure?" Though humorous, it is also a serious question, since it illustrates how easily personal data can be accessed and how easily people can be manipulated. Are products considered in terms of their potential impact on critical infrastructure?

Mr. Kolasky: We care a lot about community and business security and have therefore adopted a fairly broad definition of critical infrastructure. There are times when security dictates that we determine which elements in our critical infrastructure represent a national security concern. This determination is guided by the Section 9 List in the Presidential Policy Directive (PPD) 21. Technologies like Pokémon Go are not on the Section 9 List, in contrast to our electric utilities, which are on the list.

Mr. Mustard: The importance of educating people regarding cyber hygiene remains critical. People must be made aware of the risks inherent in using a product like Pokémon Go.

Dr. Paluru: In his industry, technology is not adopted until it has reached an acceptable level of maturity, which might require years to implement. The effort is necessary in order to prevent the introduction of instability into the grid. We want to examine software for vulnerabilities prior to implementation, and evaluate pros and cons prior to implementation. We have learned many lessons in moving data.

Mr. Webster: From the FBI perspective, we must carefully consider how information is disseminated. Using Pokémon Go as an example, if the product posed a threat to critical infrastructure, the FBI would work to inform the public about the potential risks, while being mindful not to infringe on vendor rights.

Ms. Murren: I'd like to shift the focus to outside the United States and understand how our critical infrastructure is ranked, and if there are models and steps adopted by other countries which might prove beneficial to implement in the U.S.

Mr. Kolasky: The principle way we interface with other nations is through our partners in the critical five: the United Kingdom, Canada, New Zealand, and Australia. This has enabled us to publish shared narratives. We have similar approaches on critical infrastructure policies. There are critical foreign dependencies. We have broadened our ability to share information.

We met with representatives of the Gulf countries in the Gulf Cooperation Council (GCC), who expressed an interest in obtaining U.S. technical assistance. Companies doing business on a global scale have to navigate through differing rules and expectations regarding critical infrastructure. NIST has been instrumental in providing guidance in this area.

Ms. Murren: Would their methods of creating mandates, or incentivizing cybersecurity be the same as ours, or would they differ in any way? Is there is consensus among nations concerning standards, implementation, and other concerns?

Mr. Kolasky: They are not exactly the same as ours, but there is some consensus on moving toward shared approaches.

Steve Mustard: In the United Kingdom, the Health and Safety Executive has adopted a strategy in which risk is considered in terms of its manageability rather than by enforcing strict regulations on a point-by-point basis. Member organizations demonstrate compliance if it can be demonstrated that they have carefully considered the risks and have taken measures to ensure that they are addressed.

Dr. Paluru: We in my industry have evolved from simply implementing compliance to a risk-based approach. This ensures a timely response to incidents as a priority, after which, compliance is considered. Europe has moved in this direction. The thought process now is, secure the system first and evaluate compliance later. To answer your question of where we rank in grid security world-wide, we are probably in the top five. When the Ukraine incident occurred, we went through a checklist of the security events that occurred there.

The checklist demonstrated that what happened there could not happen here, at least in the WAPA region, because we have prepared for those eventualities. General support systems and field devices run on completely separate networks with air gaps in between. We make sure data transfer is very secure. There are three different systems, so that email is separate from the others. We do not acknowledge alarms, but send crews out to the field to check. We do extensive systems checks. We do not want to be in a situation where a simple breaker failure will cause the grid to go down.

Mr. Webster: From the FBI perspective, we have cyber stations outside the country that we use as trip wires to other countries to provide information if we see something. Information travels in two ways. It can preempt attacks from outside the United States. It is the best way for the FBI to work. We tend to stay outside the realm of businesses operating outside the United States, but we try to provide some common sense security perspectives on operating in particular environments.

Ms. Wilderotter: *[to the Panel*] Since we are wrestling with the right policy recommendations for this critical topic, for each of you what would your number one policy priority be?

Mr. Kolasky: If I could legislate for a day, I would seek to facilitate cooperation between government and industry in order to work more quickly together on a range of topics. In working with industry and listening to them, I urge the commission to listen to the private sector panelists here today. There has to be a governance framework that moves us into the twenty-first century and arriving at solutions together sooner.

Mr. Mustard: Movement toward a broad implementation of risk-based management rather than by rote. Cybersecurity must be understood as one of the key risks.

Dr. Paluru: Cybersecurity Information sharing is the top priority.

Mr. Webster: I concur with Dr. Paluru's assessment.

Ms. Wilderotter: Are there specifics regarding information sharing, for example prevention, detection, or some other consideration.

Dr. Paluru: Prevention is most critical, and thus is most dependent on timely information sharing. Additionally, access to lessons learned after a breach has occurred would prove helpful. Speed in

acquiring information is crucial to securing systems. There are many modules in an energy management system, detailed information is critical to determining where events occur.

Vice Chair Palmisano [*To Mr. Webster*] I have observed that our efforts have been misaligned by taking a reactive and defensive posture. We have been concerned more with vulnerability mitigation, rather than focusing on how best to detect and prevent attacks in the first place. Mr. Webster might be in the best position to respond to how best to respond to the bad guys. The FBI has approximately 14,000 agents and asked Mark how many have been tasked to conduct critical infrastructure investigations.

Mr. **Webster**: Critical infrastructure incident investigators number between 500 and 600, or about three percent of the workforce.

Mr. Webster: The FBI forms Cyber Task Forces (CTF) largely staffed by members of local law enforcement trained in FBI investigative techniques. The agency also works closely with DHS.

Mr. Palmisano: I am still uncertain as to what the FBI is doing to proactively track the bad guys themselves. In the case of the Department of Justice, metrics are routinely published. Investigative and prosecutorial information furnished by the FBI would help the Commission to comment on a possible realignment of resources to assist in prosecuting critical infrastructure attackers. We request the FBI furnish pertinent information to the Commission regarding its success rate in investigating and prosecuting criminal attacks on critical infrastructure.

Mr. Kolaski: There have been recent indictments supported by DHS investigations in the New York area, and law enforcement is one of several efforts to prosecute and prevent CI attacks.

Mr. Webster: We can provide the Commission with more detailed metrics in a secure environment. The FBI might not be able to prosecute cases in which attacks emanate from outside the United States.

Ms. Anton: What would happen if an attacker launched a GPS-spoofer against an electrical substation? Is deploying a crew to the area within 30 minutes the best we can do? It is possible to operate all or a portion of critical infrastructure without GPS timing and synchronization?

Dr. Paluru: GPS spoofing still poses a significant threat which needs to be addressed. Like Mr. Webster, we could provide detailed information, provided it is conducted in a secure environment. The system is designed in such a way that a GPS spoofing attack could not take down the entire grid because it is interconnected. As an example, if a power generator was taken down at a particular substation, the power flow and frequency could be immediately addressed by power provided by a power generator located in another state or in British Columbia. If an attack was world-wide, or of a scale to affect the entire North American continent, the situation would be very bad.

Mr. Kolasky: Timing is the most important factor in addressing a critical infrastructure attack. He would like to see attention directed toward testing Positioning, Navigation, and Timing (PNT) service backup systems.

General Alexander: Assuming that a critical infrastructure attack has occurred against the energy grid, either emanating from or supported by a nation-state, how should the government respond, and who assumes what role?

Dr. Paluru: The grid is a "living thing." It will operate apart from cyber control systems. Some substations still have synchro-scopes – manual devices which sync a generation to the grid. In the event of a major, coordinated attack, the grid will still be vulnerable to cascading outages, but it is designed to immediately alert unaffected segments of the grid to any anomaly emanating from the affected area. We can then dispatch teams into the field to address the situation.

General Alexander: If such an attack occurred, the liability shouldn't rest with those tasked with maintaining service, but should be shouldered at the national level. I suggest this because there is a point, in such an attack, in which normal expectations are overtaken because of the scale of the attack.

Mr. Webster: As the result of tabletop exercises, the goal of the FBI is to alert critical infrastructure sectors when trends are identified on networks. The Agency strives to determine the nature of the attack, whether cyber or other, then to work with the critical infrastructure sector to remediate the situation. In the case of a catastrophic attack, policies are in place to enable the FBI to intervene when necessary.

Mr. Kolasky: In such a scenario, the federal government will assist, when requested, in threat reduction and asset response in the form of insert teams to assist in remediation. We do have a cyber response group, operating out of the White House, to oversee collaboration across agencies. We also assist in more traditional ways, such as emergency management.

Mr. Mustard: There is wisdom in distinguishing between continuity-of-operations efforts and those undertaken by law enforcement. I attended a Cyber Shield exercise conducted by the National Guard, and was impressed with the level of preparedness and training among its personnel.

General Alexander: Business and government should, collectively, practice the full spectrum of response in order to do effective tabletop exercises as is practiced in the Cyber Guard.

Dr. Paluru: In the event of a major attack on the energy grid, the Secretary of Energy is authorized to take over control of the grid in order to direct mitigation efforts in a timely and efficient manner.

Mr. Lin: [*To Mr. Kolasky*]: what are the consequences for an individual firm for being put on the Section 9 list?

Mr. Kolasky: The federal government would offer the firm whatever resources were at the government's disposal. For example, the intelligence community would furnish the firm with information specific to an actual or suspected threat against them. And before such an attack, exercises have been conducted to practice collaboration between government and business.

General Alexander: According to Mr. Kolasky, there are no downsides to being on the Section 9 list. What is the approximate number of companies currently on the list?

Mr. Kolasky The number of companies on the Section 9 list is in the two-digit range.

Mr. Lin: *[To the panel]* How do we foster a culture of security?

Mr. Mustard: There already exists a very strong safety culture. If cyber security is thought of as a safety risk, the existing vigilance can be leveraged to include cyber safety, which, at present, still needs improvement. He added that safety is commonly the number one priority of top management.

Dr. Paluru: WAPA conducts a Job Hazard Analysis (JHA) prior to conducting any work effort, and acknowledged that the same practice should apply to CS.

Mr. Webster: The FBI routinely provides business with information on how to address cyber threats and works in teams or one-on-one in order to effectively implement the effort.

Mr. Lee: Are we making the right tradeoff between innovation and availability, what might SCADA systems look like, or, what should they look like ten years from now?

Dr. Paluru: The utility industry always looks 10, 15, or even 20 years ahead. He envisions the SCADA system making most of the decisions due to the increasing complexity of integrated systems. He said that it isn't uncommon for grid operators to receive anywhere from 1,500 to 2000 alarms every hour, with its consequent impact on decision-making. Looking ahead, SCADA will assume configurations now being manually implemented. It is important to strike a balance between innovation and availability.

Mr. Mustard: The trend is toward more intelligent devices with the capability of making decisions at the local level while subject, if necessary, to human intervention. At the same time, the pace of innovation requires a robust application of risk-based analysis to manage technological change and to better inform decision-making.

Mr. Kolasky: In order to stay ahead of the pace of technological change, potential vulnerabilities must be considered when designing cyber systems. He said that development at DARPA and at universities is ongoing, but acknowledged that addressing security, while anticipating future vulnerabilities is a constant challenge.

Mr. Sullivan: From a DHS and FBI perspective, how many skilled engineers are actively engaged in development, and how much is invested in educating staff, consumers, and the public to foster cybersecurity awareness.

Mr. Kolasky: The overall budget for his group is approximately $1 billion. Within that budget, approximately $20 million has been allocated to education and $100 million toward engineering efforts. He was unsure of the amount spent for law enforcement.

Mr. Webster: The FBI competes with private industry to hire the "best and the brightest" to address cybersecurity. After training at the FBI academy, those individuals are assigned to cyber squads or to the cyber division at headquarters. Education is implemented through a private contractor. Individuals are trained in specific skill-sets, like designing and reading malware.

Ms. Todt: On behalf of Ajay Banga, how do we assess the present-day risk of technologies already in, or being designed to inform our critical infrastructures?

Mr. Kolasky: In general, companies want to share information and to reduce risk, but it takes time. We define critical infrastructures by the degree to which they contribute to our national economy. There are good business reasons to take the necessary steps, since boards and investors require such diligence.

Break

Panel 2: Critical Infrastructure Cybersecurity Challenges Affecting the Digital Economy

Scott Aaronson, Executive Director, Security and Business Continuity, Edison Electric Institute (EEI); Member of the Secretariat, Electricity Subsector Coordinating Council (ESCC)
Chris Boyer, Assistant Vice President, Global Public Policy, AT&T Services Inc.
Dr. Wm. Arthur "Art" Conklin, Director, University of Houston, Center for Information Security Research and Education
Scott Robichaux, Cyber Security CoE Manager, ExxonMobil GSC Information Management

Scott Aaronson, Executive Director, Security and Business Continuity, Edison Electric Institute (EEI); Member of the Secretariat, Electricity Subsector Coordinating Council (ESCC)

Mr. Aaronson talked about the distinction between cyber and physical security. In almost every cyber-attack, there are physical implications. Conversely, physical attacks almost always have cyber implications. These distinctions encourage a holistic view on cyber and physical security.

There are three elements of critical infrastructure security:

First, there are standards. Though they help create a foundation for security, they are static and thus cannot create security itself. While standards are static, partnerships, which evolve over time, are dynamic.

Senior executives and boards of directors recognize cybersecurity as important. An enlightened leadership is critical in creating a culture of security. They determine priorities, direct resources, and, of equal important, they attract other like-minded leaders from industry and government.

The Energy Sector Coordinating Council (ESCC) is a catalyst for leaders in industry and government to focus on three specific elements:

- Tools and technology, which fosters research and development.
- Information-sharing, making sure the right individuals get the right information and the right time.

  It also encompasses machine-to-machine information sharing and cross-sector sharing. While other sectors are dependent the flow of electricity, the power sector is as dependent on all other sectors in order to function properly. Without a steady supply of water, power cannot be generated. Without a functioning transportation system, power cannot make its way to the consumer. Without financial services, we have no access to capital markets.

- Response. The ESCC practices a lot. Dwight Eisenhower said "Plans are useless. Planning is everything." Mr. Aaronson prefers a quote by Mike Tyson: "Everybody's got a plan until they get punched in the mouth." Resilience, response, and recovery are critical. We must be right all the time. The enemy only needs to be right once.

The incident in the Ukraine was an eye-opening experience. But it was not an eye-opening experience because we knew that could happen. The incident brought up the importance of contingency planning. Over the past century, the grid was operated without any digital overlay, which means that planning must include going "back to the future", to access our systems as was done in the years prior to digitization.

A report issued by Paul Stockton from the Homeland Security Advisory Council dealt with cyber incident response and touched upon the interdependence of energy, finance, and communications. Until recently, each of those sectors planned in isolation.

Chris Boyer, Assistant Vice President of Global Public Policy for AT&T Services, Inc. He also serves as Chair of the NIST ISPAB in Washington, D.C.

The National Communications System (NCS) was founded in 1963 by President Kennedy as the result of the Cuban Missile Crisis. Mr. Boyer spoke on three recommendations:

First, the Commission should appeal to the President regarding the critical importance of the public/private partnership model and to adopt a strategy within government to eliminate duplication of effort.

Congress, the Administration, and expert agencies have recognized the partnership model as the most effective way to enhance Cyber Security (CS) as opposed to a regulatory/checklist approach. The partnership model was instrumental in the development and implementation of the NIST cybersecurity Framework and other efforts such as the DHS Sector Coordination Process and the NTIA Internet Policy Task Force.

We are seeing federal agencies adopting a prescriptive, regulatory requirements related to cybersecurity. For example, the FCC has proposed an over-broad risk-management and data security requirements scheduled for completion in the next few months. Proposals such as these are counterproductive and contrary to the approach adopted in the NIST Cybersecurity Framework. NIST believes that government, as a whole, approves of the approach adopted by the Framework.

We continue to urge policies to ensure that agencies promote the public/private partnership model. Conflicting programs create a high degree of uncertainty and distracts from joint efforts to detect and respond to actual cybersecurity threats. The public/private partnership model and the regulatory model cannot co-exist and only add to the duplication of effort in the government.

Second, the Commission should develop strategies to enhance cybersecurity in a world of converged services and technologies. As an example, the communications sector is transitioning systems from legacy to IT-based systems, such as network virtualization. The implementation of efforts such as these will only emphasize the interdependence of sectors and agencies, making public/private partnerships even more important. If agencies continue to follow a siloed path, their efforts, as illustrated by FCC initiatives, will limit the scope to only include entities which fall under single government entities.

Third, the Commission should support the development of forward-looking, strategic technology plans to enhance the nation's cybersecurity. This is critical in order to manage cybersecurity in a rapidly changing environment. To stay ahead of nation-state and other actors, the communications

sector is exploring development of digital technologies to enable a more rapid and flexible response, such as leveraging tools in the cloud. The President's National Security Telecommunications Advisory Council (NSTAC) serves as a good model to assess the implications of technology development.

Dr. Art Conklin, Director of the University of Houston's Center for Information Security Research and Education.

As a child of the space age, it is true that the innovation resulting from that environment was due primarily to people and not just to technology. They were intelligent people driven by a purpose.

As a consequence, our greatest challenges are not technical, but rather are a lack of people possessing the needed skills to address future challenges. At the same time, the challenge is that security wasn't designed into the technology. As a result, security strategies have been "bolted on" after the fact. It is like changing car parts while driving down the highway.

The problem is more complex than a lack of skilled people. Hiring skilled people is relatively easy, but what is not so straightforward is acquiring competent business and project managers to direct research and development and marketing because they drive the innovators. Even though we're living in the 21st century, our critical infrastructure was primarily engineered in the 1990s. When looking at the future, it is important to remember that these systems have very long lives.

Referring to President Kennedy's speech about sending a man to the moon, Dr. Conklin called attention to the words that followed: "and returning him safely to earth." The word "safely" made the effort much more challenging. It was also important because achieving that goal ensured that the effort would survive into the future. We need a present-day rallying cry to address the challenges facing us today. We need to build-in security at the outset of new development.

In order to address the problem of obtaining skilled people, education and training must be stressed, with a focus on where to apply the education and training. In order to experience an environment of successful education and training, one needs to go no further than the oil and gas industry. A quick way of triggering a safety alert is by walking into their headquarters with a smart phone, or walking on a stairway without using the hand rail. Safety is part of their D.N.A.

The next generation must learn our generation's lessons now, or they will learn them the hard way later. We must adopt the attitude that security is not someone else's problem, and to exercise restraint with innovation: it may be useful but it may not deliver the desired result.

Increased funding is needed to introduce Science, Technology, Engineering and Mathematics (STEM), starting in middle school, to include every technology field. We need to address the skilled teacher shortage in cyber and STEM. Schools do not have the budgets to maintain cyber programs. They must change every term to keep up. We must appeal to the President to set aside money for programs. Grant money exists, but not the related resources. People have always been our best asset. We are not asking for free fish, we need to learn to fish.

Scott Robichaux, CoE Manager for Cyber Security with ExxonMobil GSC Information Management.

Mr. Robichaux offered three aspects of the cyber security landscape in which most oil and gas companies operate.

First, computer systems which make up the industrial control systems and operate our most critical components. The threat of cyber-attack against such systems is "significant." These systems rely on computer technology at all points. It is critical that we isolate safety systems from those controlling the unit.

Second, we rely heavily on our internet-facing components such as eCommerce for product purchases, as well as in areas in which we collaborate with our business partners. We protect our internet-facing assets by creating a safety zone to control the traffic between the safety zone and our internal network.

Third, our final focus area is on our internal network on which our employees use the internet for email, collaboration, and analytics. Most of our intellectual property assets are stored here. Our cybersecurity approach is early detection, and a layered approach to defense. We also stress user awareness, since no amount of technology can protect against every threat. The end user plays a key role in cybersecurity.

Our cyber adversaries include people motivated by financial gain (such as stolen credit card information, or others), ideological protesters, to more dangerous adversaries such as nation-states interested in our intellectual property, or, in more extreme instances, the physical destruction of our assets.

Since the oil and gas industry considers protection a significant priority, the measures adopted by ExxonMobil are described below:

- High-level support for cybersecurity initiatives.
- A multi-layered defense approach is the best way to deter attacks on our critical infrastructure.
- Maintaining basic security hygiene is essential, such as ensuring that anti-virus software is up to date, timely deployment of security patches, using powerful systems of identity verification, and restricting the use of removable media devises such as USB drives and CDs and restricting access to personal webmail on company workstations.
- Conducting periodic drills (often unannounced) to ensure that threats can be detected, contained, and remediated.
- Developing plans to address worst-case scenarios.

We have the following recommendations:

- Provide the infrastructure and processes to facilitate timely and actionable collaboration and information-sharing. For industries, such as oil and gas, information-sharing should also take into account international considerations.
- Continue to promote and enhance the NIST Cybersecurity Framework as the preeminent and international standard for policy formation and implementation. The Framework addresses the five key aspects of cybersecurity: identify, protect, detect, respond, and recover.
- Before technological products and systems are deployed, to ensure that they be fully-tested for vulnerabilities and that cybersecurity is built-in and managed throughout the life cycle. It should be totally unacceptable to introduce devices into our control systems which contain known vulnerabilities.

- Take a measured and coordinated approach to new security laws and regulations, ensuring that the regulations are risk-based and not one-size-fits-all. Setting minimum standards often has a stifling effect on advances in cybersecurity technology.

Panel 2 Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Ms. Wilderotter: What initiatives could the Commission recommend in order to get resources for cybersecurity education and training throughout organizations and how do we acquire cybersecurity-savvy employees?

Dr. Conklin: Make a strong case to upper management and corporate boards that the investment is worthwhile and understandable. A cybersecurity culture should include all employees down to the janitorial staff, who might find a USB drive on the floor, and who would then know how to report the incident.

Mr. Aaronson: Everyone who has an account with ExxonMobil is required to go through a certification process. The organization also disseminates regular bulletins on cybersecurity issues. We also "gift" our employees with simulated phishing emails and monitor employee responses to what they receive. This also generates an atmosphere of competition as to who can do better.

Mr. Robichaux: Cybersecurity must be presented as a personal issue. It must become as familiar as other safety related measures people typically take. Exxon Mobil is very focused on safety awareness programs, and they find these programs are having personal impacts for many of their people in their personal lives as well. Anyone on any ExxonMobil system is required to take awareness training.

Mr. Boyer: Like ExxonMobil, all our employees go through annual training in cybersecurity and privacy. When they login, they receive notifications regarding caution on phishing, and other topics. Our security officer frequently disseminates training videos. Security is part of the day to day operations of the business. Our Chief Executive Officer stresses our Network 2020 Initiative, with training on how do we get to virtualization in the cloud, and training on new technologies.

We have developed the Tech Transformation Series, designed to education our employees on shifts in technology in the industry, among those is cybersecurity, a separate module within the series. Among our over 200,000 employees, many come from legacy systems. AT&T is focusing on retraining staff using legacy systems on new technologies. We also encourage our employees to avail themselves of certified cybersecurity courses with tuition reimbursement offered by a university with whom we have a relationship.

Mr. Aaronson: It is a cultural issue, and reflects the values of senior executive leadership. There are real ramifications to failures in phishing training. The first time any of our employees engage in spear phishing, they're talked to. The second time they lose internet privileges for a period of time, the third time, there is no third time. Showing the severity of infractions helps to change the culture going forward. Where we differ in approach is the siloes that grow up within enterprises. It's not just HR, all parties need to work together. There needs to be change with executive oversight over all these areas. Security is an enterprise-wide undertaking, and treated as part of everything that's done.

Mr. Chabinsky: *[To Mr. Boyer]***:** We always talk about the fact that industry is going to be on the front lines of cybersecurity. It is absolutely true. The problem is, industry is not being paid to be on the front lines of cybersecurity. There is a market failure there. There is no one on the frontlines more than the telecom providers, especially the Tier 1 companies. It appears that in most of the discussion that it is a foregone conclusion that everyone, down to the individual consumer or individual employee, regardless of size, needs to engage in cybersecurity. We might be able to raise this issue to a much higher level, of core providers and key providers. If cybersecurity was a profit center for Tier 1 providers and others, we can provide them with liability protections at the same time. This way we can change the dynamic.

When the nation wanted to make sure there was universal service in the United States, where markets didn't exist, we created a "Connect America" fund to make that happen. It is surprising that there isn't anything like a "Protect America" fund to handle cybersecurity in an accelerated, uniform, nationwide manner. In your experience, being with AT&T and working with the greater community, is there any merit in raising this issue and having a core set of resources in the U.S., provided with market incentives, to really clean this up before it gets down to the masses?

Mr. Boyer: First, the concept of core companies to address cyber is not new. We talked about a concept called Active Defense back in 2010 that involved the big carriers and technology companies. There were 25-30 companies grouped together that had a lot of cyber capabilities. It was the reason the information debate started at the time, to determine how to share information. The NSTAC in the recent Information and Communications Technology (ICT) mobilization report calls that out. That report is focused on cyber response, but it proposes that "ICT enablers" be established. Then there are "consequence organizations that are more downstream, that include customers and others. The concept of there being a core group is not necessarily a new one. Whether there was a market failure, I haven't determined definitely. All those companies offer security services that we sell to people to help them deal with security. Our goal remains having the capability of stopping cybersecurity attacks at the server level before they migrate. From an industry perspective it is something we can take into consideration and come back and talk to the Commission about.

Mr. Lee: [*to Dr. Conklin*] I am intrigued by the reference to moonshots. When we think of moonshots, there is a clearly accessible goal. Did they make it to the moon and did they make it back? It's a yes or no question. It gives a clear understanding of the aspiration to the nation as was expressed by the President. The other characteristic was that there was a substantial organizational commitment, tens of thousands of people, to achieve that goal. Do you think a mindset, similar to what existed for the moonshot effort, exists within the cybersecurity effort?

Dr. Conklin: It's not only an admirable, but an essential objective. As development progresses, it could be as simple as demanding that products do what they're supposed to do, and only what they're supposed to do. Anything that interacts with critical infrastructure must do so safely. As far as organizational commitment, it already exists as the education system from K-12, and in colleges and universities. They're in the business of making the future and in making STEM work, if we make it their business to make STEM work. We need to make STEM appealing, because students vote with their feet. The means exist, but the educational community as a whole needs direction and leadership to produce desired results.

Ms. Murren: Within your sectors, are there approaches that have been particularly effective which might work well in other sectors that may not have advanced as quickly as yours have in cybersecurity, and are there approaches that have not worked because they were not effective, and also *[to Mr. Aaronson]*, I'm curious about what you've learned about the incident in the Ukraine.

Mr. Aaronson: We do have standards which have worked in the cyber and physical environments. It does promote the culture and mindset of putting security first. Also, there now is a much more effective mindset among senior government and industry leaders to promote cybersecurity. The industries represented here are diverse. It is literally one big machine with thousands of owners and operators. If we don't work together, it will fail quickly. We have been fortunate to find common ground to support that system.

Regarding the Ukraine situation, a few days before Christmas in the U.S., 225,000 people in the Ukraine lost power for about 6 hours because of a well-coordinated cyber-enabled attack allegedly by the Russians. What was interesting was that six companies were attacked, four of the attacks failed. It was not a catastrophic attack, but it was a proof of concept. There were also physical components to the attack. The threat persisted for about 6 months prior to the event.

The take-away lesson is, that is what a cyber incident is going to look like. It will be launched by a sophisticated adversary. It will leave behind indications of preparation long before the attack actually occurred. The attack was also combined with an attack on telecommunications in that affected entities were subject to a denial of service, designed to confuse the monitoring of the incident by its targeted personnel. Twitter blew up during the incident and was able to provide operators an accurate assessment of where the attacks occurred. We think we know what will happen, and there are new ways to characterize what is happening in the field.

Ms. Murren: Would you go so far as to characterize Twitter or Facebook as critical infrastructure?

Mr. Aaronson: It may be amusing to think of but, I wouldn't go that far. It does bring home the fact that these technologies are integral to one another. They have become central to our way of life, and it may be a larger view of what is critically needed.

Mr. Boyer: It is somewhat frustrating that we always think of critical infrastructure in terms of putting things in boxes, whether it is, or is not critical infrastructure. Categorizing something as critical infrastructure isn't necessarily straightforward. Strictly speaking, a service is considered as critical infrastructure if its interruption or destruction would present a catastrophic failure. The reality, however, is that there is a lot of cross-over and interdependency that eludes easy definition. It creates a paradigm of competition, and does not make it conducive to working together. It might prove more profitable if all of us thought less of categories, and more about working together as one "family."

This view brings in entities like Facebook and Twitter that offer important services, and shift away from putting entities into boxes because it seems counterproductive. In terms of what's working, the NIST framework has been a huge success because it allows companies to shape their security according to the needs of the company. In terms of what's not working, regulation will not work for security. Maybe a challenge we have is, everyone agrees we need to have standards, and that eighty percent of incidents can be prevented by having standards.

The real challenge is how do we get to the last ten or twenty percent. In a company like AT&T, with many standards certifications, it still only takes one person to cause a problem. It seems things are shifting away from the protect function to the response function. The question becomes, not if but when there will be an attack. That is what the commission should think about in terms of the future. The other situation is how we deal with very sophisticated attackers we may not be aware of, and dealing with that area.

Mr. Lin: It's not clear to me that the moonshot analogy is accurate, since we can't go to the moon today. I'd like to better understand the argument against regulation per se. Regulations arise in situations in which people see a problem. We have tried to deal with it thus far with public private partnerships, and we still have a problem. My real question is: if regulation is not perceived to address the problem, is it because you don't see a problem or that regulation is not a way to address the problem? I'd like to better understand the logic of the argument.

Mr. Boyer: The presumption is that for regulation to work, people must know what to do to solve the problem. It presumes there is a set solution to every problem. In cybersecurity, the attacks are changing constantly. The risk is that companies may focus solely on regulatory solutions to an attack that may offer a slight improvement, but won't provide a real defense from an attack. Company resources will be forced to use resources to be compliant, instead of being flexible and adaptive to changing attacks. Most companies take this issue very seriously, and understand it's a problem. Regulation can divert attention from the ability to respond to changing threats, and create a rote compliance regime. Companies have demonstrated commitment to these issues.

Mr. Robichaux: It is somewhat misleading to equate cybersecurity with safety. In the latter, we have empirical proof that if maintenance isn't done, for example, on a particular valve or pump, there's a very high level of probably that failure will occur. In cybersecurity, however, we're presented with an intelligent adversary whose preparations are largely unknown to us. We don't understand their resources or capabilities, so our best approach should be in building defenses to protect our highest value critical infrastructure assets. I also maintain that if a company is truly committed to following the NIST Framework, based on a risk-based analysis of their particular company, they will be much better prepared to prevent or mitigate a cyber-attack on critical infrastructure. And since the Framework is not designed as one-size-fits-all, compliance doesn't take on the characteristics of a checklist.

Mr. Robichaux: The challenge regarding regulations is that since compliance to the NIST Framework varies depending on how it best addresses the vulnerabilities of a specific company, framing regulations in terms of language would be neither realistic nor productive.

Mr. Boyer: The Framework is interpretive and should be used to create a risk management plan specific to individual companies. From a regulatory standpoint, there will be huge differences of opinion on how the framework is applied, because it is designed to be flexible. The Framework does not mandate standards, but provides guidance in fostering cybersecurity.

Mr. Aaronson: While our industry takes regulations and standards quite seriously, we also recognize the significant shortcomings in those regulations to fully address the evolving cybersecurity landscape. There are profound shortcomings in a couple of ways. I don't know that

we can keep up with a security standard alone. One shortcoming with standards is the drain on corporate resources when those responsible for cybersecurity must also supervise compliance.

Mr. Boyer: The FTC provides a slightly different approach in expecting companies to make a "reasonable" effort to comply and that, if that effort has not been made, the FTC might use its enforcement role to ensure compliance. I don't necessarily endorse this as the path to take, but it does present a different way of looking at security. It is different from a proscriptive regime, where what must be done is explicitly defined vs the expectation that reasonable actions will be taken.

Gen. Alexander: Today, industry is responsible for preventing protecting against cyber-attacks, even if launched by a nation-state. But since the efforts of a determined nation-state will ultimately prove effective, it seems reasonable to expect the federal government to weigh in. Do you agree with that?

Mr. Aaronson: Yes, I totally agree.
Dr. Conklin: Yes.
Mr. Boyer: Absolutely.
Gen. Alexander: My second question is, if it can be shown that the entity targeted by a critical infrastructure attack has complied with existing standards, is there a legislative strategy to absolve that entity from lawsuits related to the attack itself? For instance, if the entity was attacked by a missile, they would naturally be exempt from consequent lawsuits. Can the same mechanism be introduced in the instance of a cyber-attack?

Mr. Aaronson: If it can be demonstrated that a company has taken the necessary prescriptive steps to protect itself, I do believe the federal government should step in to mitigate in the event of lawsuits.

Gen. Alexander: In other words, if a compliant company is attacked, they are not liable, agreed?

Mr. Aaronson: I agree.

Dr. Conklin: We already have Act of God, Act of War exceptions in insurance policies. In the event of an attack by a nation-state, it becomes all hands on deck. We mobilize everyone to get the affected services back up and running. Government and industry would work together in the interest of the society as a whole. That would include fallout of things that are beyond anyone's control, for either government or industry. There may need to be controlling legislation that adds "Act of War", or "Warlike" actions. It should not absolve a company necessarily, if standards were not met.

Mr. Boyer: It's quite possible that a company would use the NIST Framework as a defense if litigated against. Gramm Leach Bliley defines meeting standards as a reasonable approach. It becomes something like a safe harbor approach.

Mr. Aaronson: The insurance industry is working to exonerate a company's liability if it can be shown that requisite cybersecurity steps were taken prior to an attack. The "blame the victim" mentality in cybersecurity has been somewhat baffling. If a nation-state attacks a private enterprise, why is the private enterprise at fault in that instance? That should be what the government is for. The insurance industry is helping to identify what compliance looks like, to assist with determining company liability. Is not an attack by an advanced persistent threat,

effectively an act of war? When looked at in that construct, it becomes clearer that blaming the victim when we're under attack from an act war, the victim is not to blame.

Mr. Boyer: When an attack rises to the level nation-state, we really do need to work together with the federal government to set policy. There is work going on to figure out what the interaction with government should be.

Ms. Anton: [*To Mr. Boyer]* You have noted that a prescriptive regulatory model cannot co-exist with a public-private partnership model. In the first panel Mr. Mustard advocated for a risk based approach, and you mentioned the FTC model. Are there metrics that allow us to consistently and reasonably determine whether what an organization is doing meets the definition of reasonable? I'm struggling with how to minimize regulation and still have good cybersecurity, and also how to tackle the issue of metrics.

Mr. Boyer: The challenge is, how do you measure cybersecurity and whether efforts are adequate to meet the challenge? I don't know that we have a great handle on being able to measure. What *can* be measured is outcome. So, as a service provider, our priority is keeping our network up and running. Other aspects are more difficult to measure. We can measure indicators of attacks, but user metrics are difficult because there are many causes for problems that users experience.

Ms. Anton: Would you then advocate for a due diligence or standard of care approach?

Mr. Boyer: I wouldn't endorse that approach. If a company is blatantly irresponsible, they will, sooner or later, be found out. I'm not convinced having a prescriptive regime up front is the approach.

Ms. Anton: One of the things that makes this challenging is that security requirements vary from sector to sector. An article in yesterday's Wall St. Journal stated that cyber-related incidents on the grid must be reported in a certain number of hours. In some cases, a company or industry doesn't have the resources to enforce compliance. Even if incidents are reported, there may not be resources to follow up on those reports. We should look at the different agencies to evaluate their ability to enforce.

Mr. Aaronson: I think what can be taken away from the *Wall Street Journal* article yesterday was a focus on physical security. There is a physical security standard known as (Critical Infrastructure Protection) CIP 014. It is interesting in the context of this discussion about regulating large industries in that it is flexible, because security planning revolves around asset value. There is a regulatory flexibility built into protecting assets of differing values. Once the plan is developed, there is third party validation that assets are being protected according to the applicable plan. With respect to the Wall Street Journal article, it talks about nuisances such as thefts, vandalism, or trespassing. The title of the article was, "How America Could Go Dark". What was interesting about the article was that it described a number of incidents, but none of those included a disruption of power.

The best example of an incident involving a substation, was a shooting at a Metcalf, CA substation in 2013. Seventeen of the twenty-one transformers at the substation were completely destroyed, and the lights did not so much as blink in the Silicon Valley. It is a very resilient system. The

hypothesis that we are all going to die because of the electric grid, as stated in Ted Koppel's book and by others, completely misses the actual resilience of the electric grid.

Dr. Conklin: If we could return to metrics and measuring. We arrived at the following thought that plagues us: How do you measure education success? It is also a problem. When we look at most of our educational systems, a big piece of how success is determined over time is how we react. What we identify as broken, what do we identify as quality improvement, and how do we fix it. It is never a point in time measurement, but a look at the journey. It all works until the point in time when the audit happens. Auditors examine what is happening at a point in time. What happened leading up to that point is irrelevant from the audit perspective. Even if something is scheduled to be fixed tomorrow, it still is a finding today. One of the important parts of metrics in terms of cybersecurity is determining if they are on the right path to making improvements and corrections.

Lunch

Panel 3: Cybersecurity Challenges and Opportunities in State and Local Governments

Edward Block, CISO, State of Texas, Texas Department of Information Resources

Major General Reynold N. Hoover, Director of Intelligence for the Chief of the National Guard Bureau; Director of Command, Control, Communications, and Computers and Chief Information Officer, National Guard Bureau

David LaPlante, CISSP, CISO, Houston IT Services, City of Houston

Edward Block, CISO, State of Texas, Texas Department of Information Resources

Mr. Block is the Chief Information Security Officer (CISO) for the state of Texas and in that role has provided policy, leadership and guidance for state agencies and public institutes of higher education. There are over 160 federated agencies and public institutes of higher education in the State of Texas. Each has its own security and information technology program. It ranges from very small agencies with 2-3 people, to very large agencies with thousands of people. They are subject to multiple federal and state regulations. Over the past few years, we have conducted risk assessments for Texas agencies. We have identified seven trends to be highlighted today:

1. Retaining staff is more challenging in state government. There are smaller salaries, less resources, fewer bells and whistles. Many people come into state government, learned the trade, and then leave. Security governance in state governments is ad-hoc. Some are very good at it, others are not. Those with federal oversight are better. Those without federal oversight are not. There is no standardized identity and access management policy across agencies. If people leave, often the credentials don't get turned off or they get promoted to positions in new agencies.
2. There is a problem with data classification in state government. The State of Texas has two public information settings. By default, everything is public, unless it's specifically an exception. That's where most agencies stop. We need to understand what we are trying to protect. They are in the process of identifying what the high value systems are. They have tried to address staffing challenges by training staff.

3. Texas law on state security is authored and maintained by the CISO office. The Texas cybersecurity framework now aligns with the NIST framework. They strongly support it. They have modified the framework a bit because of the type of government Texas has.
4. Each of the 160 agencies and institutes of higher education must submit a plan to the state CISO office bi-annually. The CISO then submits a State of the State document to the Texas legislature. It provides an overview of what is being doing well, and what the challenges are. Challenges exist where there is less focus from newer technologies.
5. Some technologies are still new to the state government. We do well with cloud security, less so with mobile application development. They are not new to the private sector, but are still evolving for state governments.
6. Legacy and old, unsupported systems are an issue for state governments. There is a technology debt in state government. There are mission critical systems running on outdated or systems that are no longer supported by manufacturers. It can be operating systems, middleware, or underlying databases. It means manufacturers no longer provide security patches, so that any vulnerability that exists in the software will be there forever. States must then develop funding models to cover purchasing new technologies to cover outdated technologies. There are multiple states with the same issues with unsupported systems. Often software companies are no longer in business, and existing software cannot run on newer operating systems or databases.
7. Mr. Block also serves as cybersecurity coordinator for the State of Texas. He provides the CISO role for non-government entities and private citizens. The goal is to raise security awareness for everyone else. It is not just true at work, but in the culture of the state.

There are past and future employees, the elderly and minors, who need cybersecurity awareness and training. This training and awareness will also help to create the kind of workforce we want for the state.

Major General Reynold N. Hoover, Director of Intelligence for the Chief of the National Guard Bureau; Director of Command, Control, Communications, and Computers and Chief Information Officer, National Guard Bureau

Major General Reynold Hoover addressed the commission on the National Guard capability in the cybersecurity realm today and in the future. The challenge of protecting the cyber domain is a team sport. It is one in which the National Guard is uniquely positioned to partner with our national defense and non-DoD entities, including the private sector. The need for cyber defense partnerships becomes more apparent every day as we become more interconnected and dependent on online systems. As the level of connectedness increases, the number of targets and opportunities grow at the same pace. The roll call of government entities, trans-national corporations, small businesses and private citizens who have become victims of cyberattacks grows by the hour.

The rapid advance of technology that continues to bring convenience and networking to government, homes and businesses has also brought identity theft, cybercrimes, foreign government and industrial espionage, and attacks on critical infrastructure. The speed of technology advancement in cyberspace continues to outpace our ability to invest in defensive capabilities. The opportunity to address the President's commission today exemplifies the importance of our shared commitment in cyberspace defense and shared critical infrastructure

protection. I know I speak for the more than 400,000 women and men around the world who say, "We're always ready, always there".

As the commission looks to build a path for continued progress into the future, I would like to highlight the National Guard's important role in growing, building, and maintaining enduring partnerships. Working together the National Guard, state, federal and private sector partnerships can disrupt and prevent attacks on our collective digital infrastructure. The whole government strategy should be a partnership at the state, local, tribal, federal levels; and a partnership with the private sector all committed to working together to safeguard our economic and national security.

The National Guard and the fifty-four states, territories, and the District of Columbia, along with the Army and Air Force are no strangers to defending the homeland and partnerships. When disasters strike, governors across the country call on the Guard to bring relief. They are the community and nation's first military responders. The National Guard's role in defense cyber operations can be traced back to the preparations for the Y2K bug in 1999. At that time, we established fifty-four computer defense network teams in case there were problems at the start of the new millennium.

State governors were given the authority to command these National Guard cyber space forces just like other National Guard capabilities within their states. These teams have remained in existence, and remain a force to support capability to support domestic missions. By 2019, the National Guard cyber capability will grow to in excess of three thousand personnel across thirty-four states, beyond the level of existing cyberspace defense teams.

We have designated these teams as Defensive Cyberspace Operations Elements. The National Guard will build the skilled cyber workforce trained to the level of their active duty counterparts. Today the National Guard is active in nearly all facets of cyberspace operations. We are aligned with proper authorities to support decision makers at all levels, including state governors, active duty services and with their various commands. Guardsmen and women are in every state and territory; and because of this, we are able to develop personal relationships with friends, neighbors and colleagues.

This allows us to support cyberspace operations in careful collaboration with other U.S. departments and agencies, including the Departments of Homeland Security, Justice, and the intelligence community. We have units performing Federal Title 10 active duty missions in support of the Army, Air Force, and the U.S. Cyber Command. At the state level, National Guard personnel can be utilized under the Title 32 authority, or in a state active duty status under the governor's direction.

As a part of a layered defense, today's National Guard provides a critical cyber defense capability to the governors of all 54 states and territories, in support of the Department of Defense and other federal and state response assets. The National Guard's ability to partner with critical infrastructure owners, government entities, public and private utilities, the defense industrial base, and other non-government entities was recently strengthened by the Deputy Secretary of Defense, who signed interim policy guidance on how the National Guard can coordinate, train, advise, and assist with cyber-support services outside the Department of Defense. These new guidelines allow our cyber-defenders in the Guard serving in a Title 32 capacity, to consult with entities outside DoD in

order to protect its assets, create situational awareness, provide for DoD mission assurance requirements, and ensure cybersecurity unity of efforts.

Governors can retain their authority to activate their state National Guard to an active duty status to respond to cyber incidents or other disasters in accordance with state law. We frequently exercise these capabilities to make sure we are prepared. These exercises range from the local to the national level, and offer another opportunity to better familiarize ourselves with our private sector partners and other government capabilities, personnel, and key cyber terrain in order to enable a rapid response when it's time to call out the guard.

Let me just highlight a few of those exercises:

- Cyber Buckeye, a state-level exercise that provided National Guard leaders an opportunity to assess the Ohio National Guard's understanding and operational competency in managing cyber incidents;
- Cyber Yankee, a regional exercise that engaged cyber operations from across Federal Emergency Management Agency (FEMA) region 1; the exercise focuses on the implications of an event that cascaded beyond state boundaries, ultimately involving all six states in the FEMA region;
  Cyber Guard, a national level exercise hosted by the US Cyber Command provided a whole-of-nation training exercise on responding rapidly to a domestic cyberattack causing a catastrophic natural or man-made cyberspace disruption. This exercise also provided an opportunity for the National Guard to train with industry, our active component colleagues, and all of the relevant federal agencies; and finally,
- Cyber Shield, the National Guard's premier unclassified collective training event provides an assessment of National Defense Cyber Operations Elements in a defensively focused cyber exercise environment designed to engage our joint service and state partners.

As might be evident from our cyber-training exercises, partnerships are a key component of what we do. Just who are these National Guard cyber defenders? They are women and men trained to the same standards as our active-duty counterparts. They are employed in the private sector, in civilian government service, or in the home. When not in uniform, they are students, moms and dads, teachers, mechanics, police officers, and office workers. They are brothers and sisters, store clerks, and veterans. Whatever their profession, their cyber skills help to uniquely position the National Guard to respond quickly in situations where a federal response may not have the appropriate authority.

They're intended to set conditions for other element response elements as situations require. Soldiers and airmen living in your communities, who are committed to protecting America's interest and critical infrastructure in cyberspace. Our cyber defenders have real world experience and valuable industry training bringing their expertise from some of the top IT and Communications companies in the world. That's why we believe the National Guard is uniquely suited for its role in cyber and critical infrastructure protection operations.

Looking to the future, the Army National Guard is in the process of establishing ten traditional cyber protection teams between now and 2019. These teams will be spread across FEMA regions and have a dual-use capability to operate in a state active duty status. The first three teams are

activated in 2017, four more will be in 2018, and the remainder in 2019. These cyber protection teams will join the Army National Guard's full time 169th Cyber Protection Team that supports Army cyber and the 54 defensive cyber operation elements across the country. The Air National Guard also plays an important and integral part in DoD's in-depth defense strategy.

There will be 12 cyberspace operations squadrons geographically dispersed across the country, composed of 71 airmen each by the end of fiscal year 2018. The Air National Guard has already begun supporting the Air Force by providing operational rotations. So, what does all this mean in terms of posturing for the future cyber and critical infrastructure threats? It means the National Guard is committed to partnerships and protecting America's interests in cyberspace, just as we defend the homeland and respond to disasters or other domestic events across the country.

It means that National Guard cyber defenders are currently involved in building greater depth and infrastructure protection and many other types of cyber operations in support of the US Cyber Command, and it means the National Guard is there to provide critical cyber capabilities to the fifty-four states, territories, and the District of Columbia in support of the Department of Defense, federal and state responses, and as part of federal and state partners in a layered partner defense.

More importantly, it means our cyber assets may be shared by states and across state lines by pre-arranged mutual assistance agreements known as Emergency Management Assistance Agreement Compacts, or eMACs. It is just another way that the National Guard provides partnership capabilities when it's needed, where it's needed. I'll close here by saying that I believe we are laser focused on defending the nation in cyberspace from foreign and domestic adversaries who wish to exploit, disrupt or destroy critical public, government and private infrastructure and in building an enduring partnership to do it effectively. As a drilling National Guardsman, I am deeply honored to be part of the National Guard's cyber effort and to be here today with you.

David LaPlante, CISSP, CISO, Houston IT Services, City of Houston

Mr. LaPlante introduced himself as the Chief Information Security Officer for the City of Houston. He has been in that role for almost 2 years. In his career as an IT professional, which has spanned over 28 years, he has worked in many business sectors in both public and private organizations in manufacturing, education, health, finance, and defense to name a few. I share this only as an introduction of my experience to provide some insight into the organizations I have had the opportunity to work with, and experience some of the inherent challenges faced within many different types of businesses.

The City of Houston has 23 primary departments, which are somewhat a microcosm of numerous business sectors including, law enforcement, transportation, aviation, emergency services, health, utilities, infrastructure, finance, and obviously governmental administration. As with many organizations, although it may be more pronounced in the municipal sectors, we are cash and resource-constrained. Prior to 2013, the City of Houston did not have a clearly identified cyber security program. In 2013 the city started a project in earnest to establish a program that would ensure information systems are secure, while enabling business to function and reduce overall information security risk.

The city chose to use the NIST cybersecurity framework as its guide to developing the cyber security program. Again, as with many organizations the resources needed to understand and

implement a cybersecurity program are limited. When I started at the City of Houston, our cybersecurity department consisted of only one person, me. The resources needed are both financial, and personnel with the appropriate expertise. Through an application for funding through the Department of Homeland Security's Urban Areas Security Initiative or UASI, the grant program was primarily focused on physical security programs. We were able to submit applications to make the organization understand that cybersecurity was an important piece of cyber security protection for the Houston UASI region. We were awarded a grant fund that allowed us to begin implementation of the new cybersecurity framework. Since the focus of the UASI program is to provide resources for the protection of the entire five-county UASI region, it was our desire to not only implement the new framework for the city, but also to provide and develop resources for other organizations.

In the region, we have worked alongside a number of municipal organizations smaller by far than the City of Houston. These resources were to include lessons learned, as well as plans and templates for processes, procedures, and guidance for implementation. Initially, it was believed that we could just provide output on a disc or download of all of the information that we generated. We learned quickly that wouldn't help our regional partners. Most of those partners had some of the same challenges that the city had, as far as being resource and financially constrained.

The first basic challenge we found was creating an understanding of the need for why a cyber security program was important and needed at all. This lack of awareness is not just at an organizational level, but it exists at the basic individual level. People understand we need protection from the bad guys who physically come to our homes to break in and rob and steal, but they don't understand that similar protections are needed to protect against cyber thieves. I often hear the comment, "I don't have any information on my computer that some hacker in Europe would ever want to access". As we continue to live our lives more and more in an electronic world, more needs to be done to protect that world. Technology is a great thing, but there are risks inherent in that technology.

I was at a recent workshop discussing cybersecurity, and one of the presenters spoke about recent ad campaigns that the public is very familiar with. According to a 2013 Ad Council tracking survey of U.S. adults, approximately 96 percent have heard of Smokey the Bear. Eighty-eight percent correctly identified his picture, and seven out of ten adults were able to recall Smokey's message of, "Only you can prevent wildfires".

Another well-known awareness campaign focused on crime and personal safety in the eighties, McGruff the Crime Dog and the campaign slogan, "Take a Bite Out of Crime". A campaign about awareness on cybersecurity topics and a memorable icon that makes cyber security personal will be worthwhile. In the basic cyber security awareness training we have performed at the city, we found that when people can see how cybersecurity impacts them personally, they are better prepared to protect themselves both at home and in the workplace from cybersecurity attacks. Recently, one of Mr. LaPlante's users relayed a story about how he was able to recognize and avoid a phishing attack thanks to the cyber security awareness training.

We've recently also provided the pilot of cyber security awareness training to some of the organizations within the Houston UASI region. We're taking what we've learned that the city and

the lessons we've learned as well as the advantages we've gained with cyber security awareness, and pass it on to our regional partners.

It is our hope that this will raise the overall level of awareness for the need for cyber security protection in individual organizations and for the region as a whole, and will ultimately provide an overall reduction in cyber security risk to the region. A second base of challenges, resource constraints, and we've heard it from a number of panels, is that most municipal organizations have resource challenges for technology.

We have many technologies that are defunct, or unsupportable and there is a deficit in that area. The resource challenge that we see is both financial and of personnel, which also has a financial nature. We can't pay people what they need to be paid, or what they can be paid in commercial or industrial environments.

In municipal government organizations we are taxpayer funded and there is only so much money to go around. The resource challenge is financial and personal. Most municipalities we work with do not have dedicated security staff, and most do not have dedicated IT staff. We have many smaller law enforcement organizations that may have one officer that who acts as IT manager. These organizations may understand the need to implement cybersecurity protective measures, but don't have any idea where to start. As the city cyber security program has developed in recognition of the challenges within the region are becoming better understood.

The output being provided to our regional partners has evolved away from discs or downloads with relevant material. A set of cybersecurity tools and resources has been created and presentations, workshops, and training has been provided to numerous regional partners including regional, independent school district, county, municipal organizations, ship channel partners, and transportation safety administration to name a few.

The tools we have created as part of the program include a cybersecurity mini-assessment, cyber security control implementation interface, cyber security posture dashboard, and the cyber disruption readiness assessment tool. The cyber security implementation interface we also called CCII was the initial resource provided to the region and the project was recognized by *CSO Online* magazine as an award-winning project for 2016. We are one of 50 organizations recognized for the project.

The projects are recognized based on a number of factors including projects and initiatives to demonstrate outstanding business value and thought leadership, and exemplary value. The interface provides a step-by-step guide to take an organization through the framework implementation process, and provides access to documentation templates, boiler plates, and instructions. It is our goal to continue making improvements and additions to the tools and provide training and workshops to assist our regional partners with implementation of solid cybersecurity programs in their organizations.

We believe that by assisting our partners in this endeavor, we will be able to reduce the overall cyber security risk to the region. While we have been able to do much with the funding that has been made available to us through the UASI program; additional focus on funding for

implementation assistance for those organizations that don't have the resources would be of great benefit.

All my focus in this testimony has been on the city of Houston, and the Houston UASI region. My experience tells me that other areas of the country struggle with the same challenges. I look forward to the opportunities allowing the work we have done here in Houston to be leveraged in other areas. Thank you again to the commission for the opportunity to speak and participate in this process, and I look forward to how I might be able to participate in the future.

Panel 3 Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Ms. Wilderotter: *[to Major General Hoover]* The National Guard is one of the most unique public-private partnerships that works really well and has been around a long time. A lot of the guard are part-time people who work full time. You mentioned how you're getting three thousand people ready across the guard. Is there a way to leverage their Guard skills where they work?

Major General Hoover: We see a great opportunity to leverage guard cyber skills for the private sector and local communities. Small and large communities are in need of cyber resources. The Guard has a pool of ready trained cyber-defenders that we could place in these critical infrastructure industries in jobs. I believe a program could be developed where Guard cyber experts work in private industry, where we may be able to direct commission, similar to what we do with doctors and lawyers in the military, and bring them in as well.

The guard can operate in its Title 32 capacity and with governor activation. At the local level, people are working as hard as they can, but don't have resources. The Guard can bridge the gap between the federal government response as a whole, and the state and local level. The U.S. Cyber Command is doing great things in defense of the nation, but there is also a growing capability in the National Guard to participate and help close the gap.

It is not the first idea people think of in terms of cybersecurity. We have the interim policy guidance that allows us to train, advise, and assist non-DOD entities incidental to our title 32 training mission. That's a huge win for all of us.

Mr. Chabinsky: One of the areas we are exploring is emerging threats. In hearing all of the exercises, this group might be representative of a larger group of state and locals working with the federal government. An area of concern is purposeful interference. I'm not seeing a lot of attention being paid on driving down collection capabilities, recognizing interference events and then being able to triangulate and discover where they're coming from. Are you seeing anything different than that? The notion I think about all the time is just everything that could be impacted by interference. Is there the development capabilities and exercises that are taking into account interference events?

Major General Hoover: I will look into and provide information back to you.

Mr. Chabinsky: This may be an area for more coordination between state and federal government. It may provide opportunity for the commission.

Ms. Murren: [*To the panel*] I'm thinking about the uneven nature of evolution in some of the states and whether there's a way that either the private sector or the government could help to even the playing field to bring those that are slower to emerge, from a cybersecurity standpoint, up to where the leaders are, and also to help to advance the states that have taken a leadership role in this particular area?

Mr. Block: We have visited multiple states. Some states are doing really good work. The breadth of cybersecurity within state government shows it's hard to be firing on all cylinders all the time. The State of Arizona has done well with public-private partnership. Michigan is also doing well. We are trying to emulate some of their practices in TX. We have worked with other states where we are ahead of the game. As people were moving to the cloud, we have used the buying power of the State of Texas to leverage certain contracts, and terms in contracts, to make sure that it included security language that states need. As soon as we did that, the buyers in other states started calling us asking us for that language, so we were able to lead that way.

There are so many agencies across so many parts of the business of state government. As we try to set statewide standards, we also try to develop best practices. We end up setting a standard all can reach. The fault in all of them is that the standards are not as high as they need to be. It's not a one size fits all. The aim is to do the risk assessment, and understand where the more valuable assets are, and look at the protections around those assets. The struggle has been determining what a minimum standard should be. It's not a one size fits all.

Major General Hoover: I think in the area of cybersecurity, just like in the area of emergency management, at the state level it varies from municipality to municipality, from state to state, and in private sector industry to private sector industry. So, when we think about who's doing it really well in terms of cybersecurity, we point out the State of Michigan. Governor Snyder has really advanced the ball in terms of information sharing, and developed the cyber range for training that's available to the private sector.

It's all about partnerships. Every year they have an international cybersecurity summit. I think you heard on the first panel this morning about the importance of better information sharing. I think that is the best practice in the same arena. We need know what's going on, and we need to know when it's happening, because it's going to go quick. It's possible we may not even know it's happening until somebody in the network tells us.

Personal and professional relationships develop through information sharing and conferences -- that's when the guy picks up the phone and calls and says, "Hey, watch out for this malware", and then all of a sudden it's discovered that it's here too. So, I think in terms of a best practice, it is information sharing. I think in terms of a model to look at, it would be the State of Michigan. Governor Snyder, in addition to his efforts within his state, partners with Governor McAuliffe from Virginia. They are co-chairs of the Governor's Cyber Working Group within the National Governors Association. The two of them are really on the forefront of trying to push cyber security within the states, and at the state and local level.

The other thing in terms of best practice would be the way we respond to disasters. The national response plan describes how FEMA and the DHS respond to a disaster; we should respond to a cyber threat in essentially the same way. We ought to be responding to cyber-incidents together.

Nobody has enough money to defend themselves against the cyber threat. Nobody has enough resources alone to defend themselves. All it takes is one person on your side of the line doing something bad that takes down the network. What happens locally has national impacts.

I think in terms of a best practice we are to look at how we respond to a natural disaster where there's a tornado or hurricane the flood. We have capabilities in place and DHS is working on the cyber response which is a step in the right direction, but the impact of a cyber-attack at the local level can quickly outpace their resources and ability to respond.

Mr. LaPlante: I have had relationships with a number of other cities to pick their brains and see what they've done and what has worked within their organization, and what they've seen that doesn't really work. Again, being fairly new to my role at the City of Houston I'm still picking up on those information sharing organizations. They have been invaluable to me. The information that I'm able to pick up and use again with everything that we're trying to do at the city. even as young and immature in our cyber security program as we are, we're trying to then pass that along to the smaller regional entities to assist them as much as we can.

Mr. Lee: It has been very important to get local perspective. On the state and local issue, all of you have spoken on variations on responsibilities across entities. In the division of responsibilities across state and local entities, how do you spell appropriate division of labor between Federal and local levels, as well as the nature of these variations?

Mr. LaPlante: We have spent time on the phone trying to track down IT people, and had a difficult time, as often small companies do not have IT people. I have also worked with a county judge, whose personal computer got taken over. It makes an interesting mix. Mr. LaPlante puts federal resources in touch with local needs. We would like to be able to offer more services, but is unable to do so.

Mr. Block: It is another level of complication for the city, with local ordinances involved along with federal and state levels. We try to use as much as possible from the federal level, and state provided capabilities. We utilize Infraguard to get and share information. I don't know if the question is more, should the federal government have more responsibility, or should they have more of an ability to set requirements.

Mr. Lee: [*to Major General Hoover*] I wanted to understand a little more clearly to imagine, what are the conditions under which a governor calls the National Guard into action? Is there is specific policy that guides our governor.

Major General Hoover: There's a couple of things: First, our cyber teams have gone into states and done penetration testing. That's one aspect that we can assist with at the state level, to do things that maybe the state doesn't have the assets to do. Then, the National Guard cyber teams can come in and do system vulnerability penetration testing. That's one aspect and the governor certainly can do that in their state active duty status and Title 32 capabilities.

The governor could use cyber assets within the Texas National Guard, on the Air Force and Army side to come in and assist the City of Houston. There is a great capability. Or, it may be that the city

may see something happening and can bring in some guard assets to take a look. If the guard sees that it is really a nefarious actor, or something really bad is going on, then the guard has that bridge now to reach back to Cyber Command or Cyber Air Force, and bring in the rest of the federal government that needs to come in. The guard's role really would be the set conditions for others to come in.

Mr. Block: In my agency there are guard and reservists, who can come in on a cross training basis. They need networks to practice on, and we have a massive network. We can both win in that situation. We get the resources we need. They get an additional place to train.

Major General Hoover: When you think about that, and apply it to the private sector. If it was something really bad that happened, the private sector or even the state and local governments aren't necessarily going to want the pros from Dover to come in, or maybe they don't want the FBI to get into their sensitive information. But they know Bob, because Bob works for them in cybersecurity in his day job in the company.

They know the cyber-guy, and oh by the way, they also happen to be an Air Guardsman and he is the Cyber trained person. What better place to have someone right there to be able to make the real first response. If there's a way that we could leverage getting these people trained, equipped, and qualified, and then place them in the private sector or place them in the public sector and in the cities and states. That's a huge win for everybody.

Mr. Lee: It is an interesting concept, and it makes me think of fire departments. I wanted to comment on Smokey the Bear. That concept has been presented to us several times, because there is some interest in engaging the public in better cyber hygiene. There was earlier testimony from someone from Dropbox, that the uptake of two factor authentication among Dropbox users is less than one half of one percent, despite its undeniable benefits. Attempts to make two-factor a default for signup has a significant impact on sigh up rates. What I want to understand is, do you have specific thoughts on what an awareness campaign ought to do? What behaviors or insights, or what sort of awareness would you want a campaign of this type to guide people toward?

Mr. LaPlante: I have no great marketing ideas for cybersecurity campaign. We know from experience, from the awareness training we've done, that even simple tips we provide to those in the city have been well received. I've had people tell me they appreciate the cybersecurity awareness training we made them take. We have received positive responses from tips we've sent. People want to know what to do. Following the tips and training, they are able to apply what they learn right away.

Mr. Block: McGruff and Smokey focus on younger people. This is where the campaign would have to take place. There is a group from San Antonio, the Cyber Texas Foundation. One of their goals was to develop a K-12 curriculum, which has now been completed. It's been adopted by the Texas Education Association, and is open to all state school districts. It is more like a Drug Abuse Resistance Education (DARE) program. It fits the age group, and it starts simple, and becomes more complex. We will have to start that way as a country, in order to build the culture. We really need to start with the building blocks in K-12.

Mr. Lin: [*to Maj. Gen Hoover*] I'm having a little trouble in imagining what would happen in a major cyber event with guard being called to respond in state.

Maj. Gen. Hoover: It's a matter of who does what and when. General Alexander talked about it this morning. There is an event in the state, and the governor calls guard to active duty with the directive to determine what has happened. In their investigation, they discover the event has a large scope. They then reach back to Cyber Command, DHS, or the FBI. The National Guard's role is not to solve the problem, but to be the first responder to the incident. It is the first military response on the scene, and can set conditions for the rest of the responders to be involved. It really is no different than a natural disaster. The governors call the National Guard first to come in, and coordinate the response of the other aid that is needed.

Mr. Lin: The difference is that those events are natural. In the event of a cyber response, someone must let the guard in the door. You speak of coordination of kind with the private sector that is not necessarily needed when responding to a natural disaster.

Maj. Gen. Hoover: The governor would not activate the guard to come into AT&T assist them with a cyber response. However, the governor could call up their National Guard assets to assist cities within the state. In the case of the private sector, the governor can offer to have the guard come in and set conditions for the rest of the response. It is because the guardsmen and women are local, it creates familiarity.

Mr. Lin: [*To the panel*] How do state and local challenges in cybersecurity differ from what is faced at the federal level?

Mr. LaPlante: Some of the challenges are the same. We also assisted the Transportation Security Administration (TSA) surface support organization. There are challenges for any organization depending where they are in their security development process. They may have questions during that process, and can get assistance as needed. It is a mix.

Mr. Lin: Are there things that states and locals face, other than lack of resources that the federal government does not?

Mr. LaPlante: This might be where we remind the commission that Texas is larger than France. We do have country-sized challenges. The threats are not necessarily different, but the response may be different. Scale comes into play. If we look at cybersecurity breach insurance, we know that the State of Montano purchased it as a rider to their physical property insurance. There are 500,000 citizens in Montana. The State of Texas has 350,000 state employees. The South Carolina breach that involved eighty percent of their citizens cost fifteen million dollars to respond. If we extrapolate out to twenty-four million Texans, it becomes a sixty-million-dollar problem. There is a lot we learn from each other, but the type of government also plays into what happens.

Major General Hoover: What do we have in common? We all face a dynamic adversary that is changing by the minute. We never thought we would watch television on our phones. The technology has changed so much from brick cell phones and pagers. We are faced with such a dynamic or changing adversary, no one really knows what will happen.

Then, we are both faced with an infinite number of people who want to get into the cybersecurity business. We can't do it individually. There is not enough people in the pipeline. The challenge becomes finding the people we need to fight the threats.

Ms. Todt: When we talked about the education and awareness campaigns, what are we actually asking the campaign to address? That is where the issue lies with ad campaigns.

[*To Maj. Gen. Hoover*] Is there a Stafford Act adaptation for cybersecurity?

Major General Hoover: This is my view based on past consideration of the Stafford Act. The impact of a cyber event in a community could be no different than a physical disaster like a tornado. It exceeds the capability of local authorities to respond. In that case, why could the Stafford Act not be applied? DHS has recognized a cyber annex is needed for the cyber response plan. In the end, all disasters are local events.

Mr. Palmisano: Is it legislative constraint to take National Guard resources to form cyber response team and deal with issues?

Mr. Block: Part of it has to do with the structure of the TX state government that makes it difficult to respond. We are trying advocate making security a line item in the budget. Whatever percentage of the budget the private sector spends on security state governments spend significantly less than the corporate average. If cybersecurity is not a line item, it makes it easier to cut out of the security budget. We have also looked at the legacy systems issue. At the last session the Texas legislature passed money for updating systems. We can then start to prioritize where money should be spent.

Public Comment

Kent LandField, Intel

> In response to Kiersten's question about what it is we would want in public service announcements (PSA). If you think about what a PSA is, in the past they were targeted towards changing behavior focusing on specific things that needed to be watched for or changed. So, if we're talking about doing something similar, then why can't you look at what is the behavior that we have both within our corporate environment, and home environments that we want to try to change?
>
> One simple thing that comes to mind is although you might have to talk to Hilton about it, is just stop clicking around. You know it's amazing how you think about silly things like that but you start talking about a bear, you start talking about a dog, that are part of our PSAs you get a simple message across. It was something very, very simple and we shouldn't overthink it. We are trying to look at changing behavior.

Ms. Todt: We will confirm and approve the minutes for the Berkeley and Houston meetings in Minneapolis.

Meeting Adjourned

The meeting adjourned at 3:40 p.m., Central Time.

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Tom Donilon
Chairman
Commission on Enhancing National Cybersecurity

These minutes will be formally considered by the Commission at its August 23, 2016 meeting, and any corrections or notations will be incorporated in the minutes of that meeting.

Annex A: List of Participants

Last Name	First Name	Affiliation	Role
Todt	Kiersten	NIST	Executive Director, Commission on Enhancing National Cybersecurity
Palmisano	Samuel, J.	Retired Chairman and CEO, IBM Corporation	Commission Vice Chair
Alexander	Keith	Founder/CEO of IronNet, Former Director of the National Security Administration, and retired four-star general who headed U.S. Cyber Command	Commissioner
Anton	Annie	Professor and Chair of Interactive Computing at the Georgia Institute of Technology	Commissioner
Banga	Ajay	President and CEO of MasterCard	Commissioner
Chabinsky	Steve	General Council and Chief Risk Officer, CrowdStrike	Commissioner
Gallagher	Pat	Chancellor, University of Pittsburgh	Commissioner
Lee	Peter	Microsoft Research Corporate Vice President	Commissioner
Lin	Herb	Senior Research Scholar, Stanford University	Commissioner
Murren	Heather	Former commissioner on the Financial Crisis Inquiry Commission	Commissioner
Sullivan	Joseph	Chief Security Officer at Uber	Commissioner
Shaw	Stephanie	NIST	Alternate Designated Federal Officer (DFO), Commission on Enhancing National Cybersecurity
Mustard	Steve	Cybersecurity Committee Chair, Automation Federation	Presenter
Edwards	Marty	DHS	Presenter

Last Name	First Name	Affiliation	Role
Boyer	Chris	Assistant Vice President, Global Public Policy, AT&T Services Inc.	Presenter
Paluru	Subhash	Senior VP & Sierra Nevada Regional Manager, Western Area Power Administration	Presenter
Kolasky	Bob	Deputy Assistant Secretary, Office of Infrastructure Protection, U.S. Department of Homeland Security	Presenter
Aaronson	Scott	Executive Director, Security and Business Continuity, Edison Electric Institute (EEI); Member of the Secretariat, Electricity Subsector Coordinating Council (ESCC)	Presenter
LaPlante	David	ISSP, CISO, Houston IT Services, City of Houston	Presenter
Edwards	Marty	Director, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), a division of the National Cybersecurity and Communications Integration Center (NCCIC) in the Department of Homeland Security	Presenter
Myrick Short	Dr. Paula	Senior Vice Chancellor for Academic Affairs, University of Houston System; Senior Vice President for Academic Affairs and Provost, University of Houston	Presenter
Webster	Mark	Assistant Special Agent in Charge, FBI-Houston Division	Presenter

Last Name	First Name	Affiliation	Role
Conklin	William Arthur "Art"	Director, University of Houston, Center for Information Security Research and Education	Presenter
Robichaux	Scott	Cyber Security CoE Manager, ExxonMobil GSC Information Management	Presenter
Block	Edward	CISO, State of Texas, Texas Department of Information Resources	Presenter
Hoover	Major General Reynold N.	Director of Intelligence for the Chief of the National Guard Bureau; Director of Command, Control, Communications, and Computers and Chief Information Officer, National Guard Bureau	Presenter
Chalpin	JP	Exeter Government Services	Meeting Staff
Drake	Robin	Exeter Government Services	Meeting Staff
Smith	Matt	G2, Inc.	Meeting Staff
Salisbury	Warren	Exeter Government Services	Meeting Staff
Norton	David	FERC	Attendee
Mario	Chiock	Schlumberger	Attendee
Castillo	Matthew	UH UIT	Attendee
Tong	Simon	Schlumberger	Attendee
Morris	Don	CenterPoint Energy	Attendee
Barrett	Matt	NIST	Attendee
Mahn	Amy	DHS, NIST	Attendee
Amin	Faisal	Berkeley Research Group	Attendee
Comstock	Norman	Berkeley Research Group	Attendee
Clifton	Douglas	EY	Attendee

Last Name	First Name	Affiliation	Role
Gurkan	Deniz	University of Houston	Attendee
Macias	Vic	National Guard Bureau	Attendee
Cressey	Roger	Liberty Group Ventures	Attendee
Kever	Jeannie	University of Houston	Attendee
Stine	Kevin	NIST	Attendee
Romine	Charles	NIST	Attendee
Dodson	Donna	NIST	Attendee
Sedgewick	Adam	NIST	Attendee
Armstrong	Robert	DIR	Attendee
Mesker	Kenny	Chevron	Attendee
Dawrer	David	The MITRE Corporation	Attendee
Dickerson	Mary	University of Houston	Attendee
Steagall	Allen	Accenture	Attendee
Trusty	Delwyn	Accenture	Attendee
Dominguez	Jake	FMC Technologies	Attendee
Navarez	Mel	Centerpoint Energy, Inc.	Attendee
Dietrich	Glenn	UTSA (University of Texas, San Antonio)	Attendee
Blackwell	Theresa, G.	Virtuo Group Corp/City of Houston	Attendee
Gomez	Jonathan	HCC	Attendee
Padilla	Aaron	American Petroleum Institute (API)	Attendee
Sachwani	Sadiq	U.H., Sugarland	Attendee
Rosney	Mark	U.H., Sugarland	Attendee
Ruffolo	Marisa	Chevron and API	Attendee
Huewemeier	Jennifer	University of Houston, Downtown	Attendee
Haynh	Nathan	Methodist	Attendee
Reynr	Paul	Booz Allen Hamilton	Attendee
Lowe	Stan	Booz Allen Hamilton	Attendee

Last Name	First Name	Affiliation	Role
Zuldema	Liz	Microsoft	Attendee
Prochaska	Joel	Enbridge	Attendee
Ernst	Martin	SLB	Attendee
Garza	Jon	University of Houston, Downtown	Attendee
Ortiz	Greg	UH Media Relations	Attendee
Lindsey	Shawn	UH Media Relations	Attendee
Ronorst	Aaron	UH Media Relations	Attendee
Swindle	Julia	Center for Offshore Safety, API	Attendee
Potter	Bruce	KeyW	Attendee
Langford	Alison	ExxonMobil	Attendee
Saber	Samir	Houston Community College	Attendee
Shaw	Ed	Self	Attendee
Hunt	Courtney	University of Houston, DOR	Attendee
Huang	Stephen	University of Houston CS	Attendee
Caesa	Wendy	Houston Housing Authority	Attendee
Villela	Marlene	Alvarez & Marsal	Attendee
Mayer	Robert	US Telecom Association	Attendee
R.	Bhagavi	Student, University of Houston	Attendee
Anderson	Gregory	Graduate Student, University of Houston	Attendee
Ledesma	Kate	DHS	Attendee
Cubbler	Scott	DHS	Attendee
Nguyen	Tim	BHP Billiton Petroleum	Attendee
Bronk	Chris	University of Houston	Attendee
Schlemeyer	Lynn	Texas A&M University	Attendee
Raosopir	Daniel	Texas A&M University	Attendee
Gause	Stewart	NRG	Attendee

Last Name	First Name	Affiliation	Role
Goenka	Nat	Not legible	Attendee
Thursten	Matt	Booz Allen Hamilton	Attendee
Landfield	Kurt	Intel	Attendee
Zhang	Yue	Aramno Services	Attendee
Loanes	Cynthia	Rowan Companies	Attendee
Lafleur	Carson	Red Tiger Security	Attendee
Wolfe	Evan	Crewell&Mooring	Attendee
Singleton	Scott	Kadeum Strategies	Attendee
Huerta	Carlos	Eastwood Academy	Attendee
Williams	Gerard	Lyondrell Basrell	Attendee
LI	Dan	University of Houston	Attendee
Jyebji	Abeerav	Shipwin	Attendee
Ritchey	Philip	Texas A&M University	Attendee
Conklin	Susan	Waashower	Attendee
McNee	T.	UIT	Attendee
Chambers	Charles	UH-UIT	Attendee
Nugz	Harvey	4IT Security Government and Compliance	Attendee
Not legible	Mario	Texas… not legible	Attendee
Cheng	Victor	University of Houston	Attendee
Ronan, P.E.	Steve	NWTS	Attendee
Gomez	Camilo	CGI	Attendee
Olson	Eric	HPD	Attendee
Parliman	Richard	LR	Attendee
Konstantinidis	Ioannis	University of Houston	Attendee
Dally	Glenn	Spectra Energy	Attendee
Morthy	Asha	Mantro Tech	Attendee
Garoia	Michael	Rowan Companies	Attendee
Boeckman	Brian	University of Houston	Attendee

Last Name	First Name	Affiliation	Role
Coulter	Braelyn	University of Houston	Attendee
Esubeur	Claudia	DIR – State of Texas	Attendee
Zacher	David	OWG-ISAC	Attendee
Pollet	Jonathan	Red Tiger Security	Attendee
Fin	Colin	University of Houston	Attendee
Lockett	Patrick	University of Houston	Attendee
Vena	Unresh	Blue Lanes	Attendee
Harris	Steph	Calpine	Attendee
Mousari	Milad	EIT Consulting	Attendee
Nieselow	Alex	MasterCard	Attendee
Byrd	Chris	EY	Attendee
Templeton	Stacy	Scalable Solutions Consulting	Attendee
Vogt	Peter	Cloud Security Alliance Chair	Attendee
Taylor	Simon	Glasswall Solutions	Attendee
Jeyanti	Yasi	Shipcon Wireless	Attendee
Tyerji	Ouresh	Shipcon Wireless	Attendee
Klump	Edward	Energy Wire	Media
Houser	MG	National Association of Broadcasters (NAB)	Media
Eaton	Collin	Houston Chronicle	Media
Weber	Rick	Inside Cybersecurity	Media
Fehling	David	KUHF	Media

Annex B – Public Participation Statements

Seven written statements were submitted by one member of the public. Copies of these written statements are available for public inspection and copying, subject to the Freedom of Information Act (5 U.S.C.A. § 552) (FOIA), at http://www.nist.gov/cybercommission/".