COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

Meeting of the Commission on Enhancing National Cybersecurity

PANELIST AND SPEAKER STATEMENTS

University of Houston

Houston, Texas

July 14, 2016

Table of Contents

Scott Aaronson

Chairman Donilon, Vice-Chairman Palmisano, and distinguished members of the Commission, I want to thank you for the opportunity to provide input on this important topic. My name is Scott Aaronson, and I am Executive Director for Security and Business Continuity at the Edison Electric Institute (EEI).

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans, operate in all 50 states and the District of Columbia, and directly and indirectly support more than 1 million American jobs. EEI has 70 international electric companies as Affiliate Members, and 270 industry suppliers and related organizations as Associate Members. For EEI's member companies, securing the energy grid is a top priority; I appreciate your invitation to discuss this important topic on their behalf.

In addition to my role at EEI, I also serve as part of the Executive Secretariat for the Electricity Subsector Coordinating Council (ESCC). The ESCC is comprised of the chief executive officers of 21 energy companies and 9 major industry trade associations. This group—which includes all segments of the electric power industry, representing the full scope of electric generation, transmission, and distribution in the United States and Canada—serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC has been held up by the National Infrastructure Advisory Council as a model for how critical infrastructure sectors can more effectively partner with government. In fact, the ESCC has been a catalyst for major initiatives that are improving the security posture of the industry and, by extension, the nation.

Cybersecurity is often looked at through the lens of information technology, economic crimes, exfiltration of data, and business disruption—concerns the electric sector shares with other members of the digital economy. However, as owners and operators of some of the nation's most critical infrastructure, our priority is protecting operational technology and preventing power disruptions that can impact national security and civil society. With this unique perspective, I would like to highlight the following topics for the Commission's consideration:

Regulatory Standards Provide a Foundation

Security standards and regulations are important to the industry's security posture.

Under the Federal Power Act and with Federal Energy Regulatory Commission oversight, the electric power sector is subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties of up to $1 million per violation per day.

These mandatory standards continue to evolve with input from subject matter experts across the industry and government. Versions 5 and 6, which became enforceable on July 1, 2016, are more rigorous than past versions, not only increasing the scope of the standards, but also adding several new requirements that mirror best practices in cybersecurity.

The industry also is applying the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Department of Energy's Cybersecurity Capability Maturity Model (C2M2). Companies throughout the industry are assessing their cybersecurity capabilities against this framework and capability maturity model and, based on results, prioritizing their investments to strengthen cybersecurity.

While regulations and standards provide a solid foundation for strengthening the industry's security posture, they alone are insufficient. As the threat environment evolves, so must the industry's security efforts.

Government-Industry Coordination

A more dynamic approach to security requires partnering closely with government, including our Sector Specific Agency (the Department of Energy, with which we enjoy a particularly close working relationship), national security and law enforcement agencies, and at the state and local level.

Protection of critical infrastructure is a shared responsibility between the government and industry. The ESCC was formed to help coordinate these efforts and to ensure we are appropriately deploying each other's expertise, capabilities, and assets. As noted earlier, the ESCC consists of energy company CEOs and trade association leaders who represent all segments of the electric sector and actively partner with government executives to prepare for, and respond to, national-level incidents or threats to critical infrastructure.

A key characteristic of the ESCC is executive engagement. In addition to providing resources and accountability that have pushed both the government and industry to work very closely and very quickly, senior executives on both sides also help to ensure unity of effort and unity of message among their organizations. During an incident, the ESCC's role—while not operational—is to provide situational awareness, coordinate with government on response and recovery efforts, and align messaging.

The industry and government leaders are focusing on four main areas that improve the security posture of the industry and the nation. They are:

> Tools & Technology: Deploying government-developed technologies that improve situational awareness and enable machine-to-machine information sharing;
>
> Information Flow: Making sure actionable intelligence and threat indicators are communicated to the right people at the right time;
>
> Incident Response: Planning and exercising to coordinate responses to an incident;
>
> Cross-Sector Coordination: Working closely with other interdependent infrastructure sectors to ensure all are prepared for, and can respond to, national-level incidents.

Risk Management; Not Risk Elimination

Instead of trying to achieve the impossible task of protecting every asset from every threat, the electric sector sets priorities to protect the most critical energy grid components against likely threats; to build redundancy into the system to make it more resilient; to coordinate preparation and response efforts with the government; and to develop contingency plans for response and recovery if grid operations are impacted.

Building on the industry's long history of mutual assistance and partnership to restore power after major outages, the electric sector is organizing itself around a Cyber Mutual Assistance program to pool resources in the face of incidents that exceed the capacity of individual companies to respond. In its early stages now, a framework is being developed to identify and share resources during incidents. Over the long-term, this project—with the backing and leadership of senior industry executives—will evolve based on the cyber incident response needs of the industry.

Another opportunity to enhance resilience includes contingency plans for operating in a degraded state. While lack of digital control or automation is inefficient and limits situational awareness, the industry is keenly aware of its impact on society and the need to keep electricity flowing. Although digital infrastructure plays an important role in the modern energy grid, the grid functioned for most of the 20th century without the benefit of Supervisory Control and Data Acquisition communications or other cyber assets. To this end, the industry is exploring the viability of deploying various low-technology or manual operating measures as part of a response to attacks on digital (automated) systems.

Acknowledging the Insider Threat

Based on experience and briefings from law enforcement, the sector recognizes that threats can come from within an organization. There is an increased focus on identifying behaviors, developing insider threat programs, and coordinating departments within companies (e.g., security, legal, and human resources) to better protect our infrastructure and operations.

A specific policy request to improve grid security is to develop a more efficient government-sponsored background screening program for prospective and current personnel with access to critical assets.

Securing the Supply Chain

The integrity of the information and communications technology (ICT) supply chain is important to the operation and reliability of critical infrastructure. A compromise of this integrity can result in the delivery of a product with malicious functionality. Similar to other risks, the ICT supply chain risk cannot be fully mitigated, but it can be managed.

This risk certainly cuts across sectors, but also across functional and organizational boundaries within an organization, touching multiple activities throughout the procurement cycle. While much of the responsibility for ICT supply chain integrity falls on the cyber asset manufacturers, the end-users bear much of the risk.

Support from government to help protect the supply chain, testing of components similar to an "Underwriters Laboratory" model, and better collaboration across the critical sectors in concert with manufacturers are all important opportunities for managing the ICT supply chain risk.

Conclusion

Effective security measures cannot be static; threats evolve and so must we. The electric sector recognizes this fact as demonstrated by the ongoing development of regulatory standards; the high-level partnerships developed under the ESCC that are enabling us to accomplish more in less time; and the focus on constantly improving preparedness by applying lessons learned from exercises and real-world events. As industry and government leaders improve their ability to protect critical infrastructure from all types of threats, we appreciate the Commission's support in this important mission.

Edward Block

Summary

The Department of Information Resources (DIR) manages the enterprise security program and coordinates statewide cybersecurity efforts through security services, policy and assurance, risk management, and education and training. Over the last several years, DIR has made progress in improving the state's overall cybersecurity posture thought implementation of multiple initiatives, including:

- Offering third party security assessments,
- Developing a unified cybersecurity framework, which is aligned to federal and private sector best practices and standards,
- Offering products and services through the cooperative contracts program,
- Implementing a shared use governance, risk and compliance software tool, and
- Providing numerous training and education opportunities.

These initiatives combined with recent legislative requirements for agencies have brought the importance of cybersecurity to the forefront; there are still several ongoing challenges however. Recruiting and retaining a workforce in the security field, disparate security services and tools, legacy systems across the state, weak information sharing, and ensuring each individual employee is trained and educated on daily cyber risks continues to be a challenge.

Third Party Assessments

For the past several years, DIR has performed security assessments of state agencies, using a third party vendor. Approximately 50 agencies had the assessment performed to evaluate their overall cybersecurity posture. Based on these assessments, seven trends were identified:

- Information security and cybersecurity staffing challenges
- Absence of secure software development standards
- Security governance and awareness is performed ad-hoc
- Manual, agency exclusive Identity and access management solutions
- Lack of 24x7 event monitoring and analysis
- Network segmentation to segregate high-value assets
- Lack of data classification policies

DIR has addressed or is in the process of addressing all of these issues, though staffing remains the most difficult issue to address.

Insufficient levels of staffing and skills focused on security and risk management: Agencies are required by Texas Administrative Code § 202 to have an established information security officer (ISO) to lead their security programs. Some larger agencies also have a core group of individuals with a combination of full or part-time security-related responsibilities. In most cases, these resources are focused on operational-oriented aspects of security, primarily network security. While a secure network perimeter is necessary and remains a foundational element of a defense-in-depth security architecture, experts generally agree that technology – and the ways the technology is being employed – has exceeded the ability of the network perimeter to provide, on its own, effective and comprehensive protection. A challenge to the ability of agencies to broaden their security focus is the lack of sufficient resources to perform the other governance and operational functions that comprise a comprehensive defense-in-depth security architecture. Some of these other security aspects include

system development lifecycle, change management with assurance processes, vulnerability and incident response management, policy and standards management and maintenance, comprehensive disaster recovery planning, awareness and training management, and regular risk assessment and management.

When agencies lack the necessary skills and sufficient number of security personnel, difficult choices must be made on areas of focus, leaving others uncovered or covered to a lesser degree.

As discussed further in the Education and Training section, DIR has developed an "Infosec Academy" to ensure state agency Information Security Officers have the necessary skills to evaluate security risks in the framework of Texas rule and established policy.

Secure software development: the department is preparing a request for offer (RFO) to deliver managed application services through the statewide technology centers. This would allow agencies to contract for software development through a standardized and shared mechanism managed similar to the way data center services (DCS) are delivered today.

Standards in security governance and awareness: In 2015 DIR, working with a committee of information security professionals from state agencies, institutions of higher education, and the private sector, repealed and replaced Texas Administrative Code § 202 (Information Security). TAC § 202 is the rule which sets statewide information security policy. The previous version of TAC § 202 was in need of restructuring to keep pace with technology. The revised version of TAC § 202 resembles the Federal Information Security Management Act (FISMA), prescribing the roles and responsibilities of state government. Technical controls are incorporated by reference and are not in the rule itself, which greatly facilitates future rule maintenance. These controls are in the form of a standards catalog that is based on the National Institutes of Standards which represents a strong, industry reviewed approach to securing information resources.

Identity and access management standardization: SB 1878 (84R) authorized DIR to conduct a study on new identification and access technologies that may better protect personal information held by the state. That study is ongoing with a report due to state leadership in November 2016.

Event monitoring and analysis: To provide 24x7x365 monitoring and analysis in a cost effective manner, DIR is preparing a RFO to deliver managed security services providers through the Statewide Technology Center program. This would allow agencies to contract for security services through a mechanism managed similar to the way Data Center Services are delivered today.

Network segmentation: Network segmentation is a process by which like systems are assigned to logical groupings based on a risk assessment of the system and information it contains. Through proper segmentation systems that contain only "public" data are kept apart from systems holding regulated, confidential, or personally identifying information. In a properly segmented network security controls can be applied most efficiently and effectively. Adequate network segmentation is based on data classification, which must be in place before segmentation decisions can be made.

Data classification: In 2014 the department published a whitepaper and template that agencies can use to develop a data classification program. Data classification ensures that resources are spent efficiently, protecting information to its requirements, rather than spending resources protecting all information to the same level. As an example, publically identifying information, whether deemed PII by Texas law or a federal regulation, has very different handling and protection requirements from information which is public in nature. By classifying data properly, risk based decisions can be made as to the protection levels necessary.

Cybersecurity Framework

The 83rd Legislature tasked DIR with developing a unified Cybersecurity Framework. The elements that comprise the Framework are:

- **TAC 202**: In 2015 Texas Administrative Code § 202 was revised and adopted. The revised TAC aligns state government with the Federal Information Security Management Act, known as FISMA, and the National Institute of Standards and Technology, known as NIST, security standards and guidelines for Federal systems. FISMA was updated in 2013 (as mentioned above).

  DIR worked with the Statewide Information Security Advisory Committee to revised TAC 202 to move it closer to FISMA and NIST. The revised TAC covers agency responsibilities and includes a Control Standards Catalog.

  - **Control Standards Catalog**: This was initiated by DIR to help agencies implement security controls. It specifies the minimum information security requirements that agencies must employ to provide the appropriate level of security relevant to level of risk.
  - **Control Crosswalk**: This crosswalk maps TAC 202 to industry standards, regulatory requirements, and compliance mandates. It allows agencies to consolidate a lot of steps. For instance, many agencies must meet state requirements, federal requirements, and even certain industry-specific requirements. With the Control Crosswalk, agencies can see at a glance how those requirements intersect and begin to prioritize efforts.

- **Agency Security Plan**: SB1597 83(R) requires each state agency to submit a security plan to DIR by October 15 of each even-numbered year. SB34 84(R), in turn, requires DIR to use the submitted plans to prepare a report concerning the State's information security posture. The structure of the Agency Security Plan template developed by DIR was created through collaboration between government and the private sector. It uses a common language to address and manage cybersecurity risk in a cost-effective way, based on business needs, without placing additional regulatory requirements on agencies. The template is divided into the five concurrent and continuous functions, initially developed by the National Institutes of Science and Technology (NIST): Identify, Protect, Detect, Respond, and Recover.

  - **Vendor Alignment Tool**: DIR also created a tool that enables vendors of security products and services to align their offerings to the Cybersecurity Framework.
  - **Guidelines and Whitepapers**: DIR developed several guidelines and whitepapers to provide more resources and insights to help you manage the complexities of information security.

Security Services

DIR offers cybersecurity products and services in Cooperative Contracts through vendor partners.

- **Network Security Monitoring, Alerting, and Analysis Services**: Provide early warning for attempted intrusions and cyber-attacks, as well as alerts to authorities that facilitate appropriate countermeasures. Advantages include: saves time with event correlation, integrates security analysis, saves money through reduced risk, meets audit requirements, and prevents attacks and provides early warning.
- **Network Intrusion Prevention Service**: Proactively identifies and blocks known threats to network security. It not only watches network traffic, but also takes immediate action based on the network administrator's set of rules.
- **Testing Services**: Offered by DIR at no cost, but entities must specifically request them. Includes Controlled Penetration Testing, Web Application Vulnerability Scanning, and Vulnerability Scan.

Education and Training

- **Texas InfoSec Academy**: DIR offers security training classes (both in-person and online) tailored to the needs of Information Security Officers within state agencies.

- **Texas Cybersecurity Council**: Building on a recommendation from the TCEEDC report "Building a More Secure and Prosperous Texas", the TCC brings both public and private sector IT leaders together to address cybersecurity education and workforce development issues.
- **DIR Cybersecurity Newsletters**: DIR publishes monthly newsletters covering security topics and outlining ways to improve individual security programs.
- **Statewide Information Security Advisory Committee (SISAC)**: Created by DIR and is made up of ISOs from state and local government and representatives from private industry. It aims to cross-pollinate ideas and best practices among its members and make recommendations to DIR for more effective information security operations.
- **Security Awareness Tools**: DIR provides end-user level security awareness training (online) to agencies that request it.
- **CIAS Monthly Tabletop Exercises**: DIR offers monthly tabletop security exercises in partnership with the University of Texas at San Antonio's Center for Infrastructure Assurance and Security (CIAS). These exercises are free for agencies.

The SPECTRIM Portal

To help tie together the overall state security program, DIR has implemented a governance, risk and compliance (GRC) software tool available to all agencies. This system, the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management, gives each agency a full view of their security posture and provide the state CISO a holistic view of statewide cybersecurity. The GRC portal provides:

- **Incident management**: requires agencies to provide timely reporting of certain types of security incidents to DIR. Timely reporting is required (preferably within 24 hours) for incidents that propagate to other state systems, result in criminal violations and need to be reported to law enforcement, and involve disclosure of confidential data (i.e. sensitive personal data).
- **Analysis and risk assessment analysis**: TAC 202 requires all agencies and institutions of higher education to perform a risk assessment. DIR, through the GRC portal, is providing a standardized method for performing these assessments.
- **Agency Security Plan**: As described above, agencies must submit to DIR a security plan each even-numbered year. To make the aggregation, review, and analysis of these plans more efficient, DIR leverages the Governance, Risk and Compliance tool to collect and analyze agency plans.
- By the Spring of 2016, the portal will also provide:
    - A dashboard that allows organizations to evaluate their security stance and compare their program's maturity to that of other agencies of similar size or mission
    - Comparison statistics for incident management and response
    - Applications for agencies to manage policies and policy exceptions

Issues Affecting Statewide Cybersecurity

- **Employee training, awareness, and education**

  In its 2015 Data Breach Investigations Report, Verizon stated that "more than two-thirds of incidents that comprised the Cyber-Espionage pattern have featured phishing." Phishing is a form of attack that uses emails to trick victims into downloading malicious code, visiting a malicious website, or entering their credentials. In 2012 the state of South Carolina's Department of Revenue was the victim of a phishing attack, resulting in the loss of personally

identifying information of 80% of its citizens and costing the state more than $15 million. Most phishing attempts are not detected by standard Anti-virus. The best method to prevent this type of attack is through user education and training.

- **Workforce development**

  Nationwide, there is a shortfall of trained cybersecurity professionals. In some areas there is a negative unemployment rate (meaning there are more jobs available than job seekers.) DIR is working to strengthen the Texas cybersecurity workforce through several initiatives outlined below.

- **Legacy Systems**

  "Legacy Systems" are information resources that are no longer supported by the manufacturer. These systems may seem to function correctly, but, since security patches and fixes are no longer available from the manufacturer, they create vulnerability in the statewide network. Without the funding to continually refresh information resources, the technology debt continues to build.

- **Information Sharing and Collaboration**

  As a federated form of government, each agency and institution of higher education has their own security function. Many of these agencies have tools and technologies to counter cyber-threats. Through information sharing and collaboration among entities the benefits from these tools is multiplied.

Chris Boyer

Chairman Donilon, Vice Chair Palmisano and distinguished members of the Commission, thank you for providing the Communications Sector and me personally an opportunity to appear before you today to provide our thoughts on enhancing cybersecurity as we move into the next Administration and beyond.

My name is Christopher Boyer and I serve as Assistant Vice President of Global Public Policy for AT&T Services Inc. In that capacity I also serve on the Executive Committee and am the former Vice Chair of the Communications Sector Coordinating Council (CSCC), which represents the Broadcasting, Cable, Satellite, Wireless and Wireline segments under the Department of Homeland Security (DHS) Critical Infrastructure Partnership Advisory Council (CIPAC). The CSCC facilitates physical and cybersecurity coordination and planning activities among the private sector and federal, state, local and territorial and tribal governments.

I also serve as the Chairman of the National Institute of Standards and Technology (NIST) Internet Security and Privacy Advisory Board (ISPAB), a Federal advisory committee responsible for identifying emerging managerial, technical, administrative, and physical safeguard issues related to information security and privacy for Federal agencies. I am also AT&T's Point of Contact (POC) representing AT&T's executive member of the National Security Telecommunications Advisory Council (NSTAC), a Federal advisory committee tasked with providing advice to the President on matters of National Security and Emergency Preparedness (NS/EP). These roles provide me with unique insight into the sector's cybersecurity priorities and concerns, as well as to cross-sector concerns.

I would like to start by providing some background on the extensive partnership that exists between the Communications Sector and the Federal government to address cybersecurity and other matters of national security and emergency preparedness. Our legacy dates back to the 1963 with the creation of the National Communications System (NCS), which President Kennedy established following the Cuban Missile Crisis to develop critical programs and plans to protect the nation's communications infrastructure. In our view, this lengthy history distinguishes the Communications Sector from most other critical sectors. The strong bond between the sector and the federal government continues largely because of three organizations that have been created in response to earlier threats to the nation's critical infrastructure. Collectively, these organizations, in concert with DHS, which serves as the Sector Specific Agency (SSA) for the Communications Sector, provide the policy, planning and operations framework necessary to address the nation's communications priorities.

- **Policy - National Security Telecommunications Advisory Committee (NSTAC).** The NSTAC (wwwncs.gov/nstac/nstachtml) was created in 1982 by Executive Order 12382. NSTAC is comprised of up to 30 chief executives from major telecommunications companies, network service providers, information technology, defense contractors and aerospace companies. Through a deliberative process, NSTAC's members provide the President with recommendations intended to assure vital telecommunications links through any event or crisis and to help the U.S. Government maintain a reliable, secure, and resilient national communications posture. Key areas of NSTAC's focus include: strengthening national security; enhancing cyber security; maintaining the global communications infrastructure; assuring communications for disaster response; and addressing critical infrastructure interdependencies. Recent reports to the President have addressed Information and Communications Technology (ICT) Mobilization in response to a large scale cyber-attack, the use of Big Data Analytics (BDA) in emergency response, including for a cybersecurity incident, and recommendations on how to help better secure the Internet of Things. Each of these reports may be useful to the Commission as they consider some of these topics in relation to cybersecurity.

- **Planning - Communications Sector Coordinating Council (C-SCC).** The C-SCC (www.commscc.org) was chartered in 2005 to help coordinate initiatives to improve the physical and cyber security of sector assets; to ease the flow of information within the sector, across sectors and with designated Federal agencies; and to address issues related to response and recovery following an incident or event. The 40 members of the C-SCC broadly represent the sector and include cable, commercial and public broadcasters, information service providers, satellite, undersea cable, utility telecom providers, service integrators, equipment vendors, and wireless and wireline owners and operators and their respective trade associations. The C-SCC and IT Sector Coordinating Councils maintain close coordination on a range of policy and operational initiatives.
- **Operations - National Coordinating Center for Telecommunications (NCC) Communications Information Sharing and Analysis Center (C-ISAC).** In 1982, federal government and telecommunications industry officials identified the need for a joint mechanism to coordinate the initiation and restoration of national security and emergency preparedness telecommunications services. In 1984, Executive Order 12472 created the NCC. This organization's unique industry - government partnership advances collaboration on operational issues on a 24 X 7 basis and coordinates NS/EP responses in times of crisis. Since 2000, the NCC's Communications Information Sharing and Analysis Center (C-ISAC), comprised of 51 industry member companies, has facilitated the exchange of information among government and industry participants regarding vulnerabilities, threats, intrusions and anomalies affecting the telecommunications infrastructure. Weekly meetings of industry and government members are held to share threat and incident information. During emergencies, daily or more frequent meetings are held with industry and government members involved with the response effort.

Members of the communications industry also participate voluntarily in a variety of other initiatives, including, but not limited to, the FCC's Communications Security, Reliability and Interoperability Council (CSRIC), the National Security Information Exchange (NSIE), industry lead security organizations such as the Messaging Anti-Abuse Working Group (M3AAWG) and a variety of other fora that share the goal of enhancing cybersecurity. Indeed, the Communications Sector is a staunch supporter of the voluntary, public-private partnership embodied by these and other organizations.

Even as we engage in these cooperative efforts, however, a principal area of concern for the sector is that we continue to see an increasing interest among certain agencies in the Federal government on prescriptive regulatory responses to cybersecurity threats. In our view, such efforts are misplaced, and in fact counterproductive. Given the constantly evolving nature of the threat, cybersecurity does not lend itself to a checklist or mandated solution. Protecting against cyber threats is a risk management function, and there is no one size fits all solution for all companies. To the contrary, a prescriptive regulatory "solution" would simply set a lowest common denominator bar that would create a disincentive for the innovation and agility needed to respond to an environment that is characterized by nimble and sophisticated hostile actors and constantly-evolving threats.

That dynamic is one reason the NIST Cybersecurity Framework has been successful as a mechanism for responding to that environment. It recognizes the diversity of companies and the need for flexible and evolving solutions, and allows companies large and small to tailor the Framework to their specific business needs commensurate to their risks. Many members of Congress, the Administration and other portions of government have recognized this model as appropriate to address cybersecurity. In fact, the U.S. government is promoting the voluntary, risk management approach espoused by the Framework internationally as an effective model to ward of more regulatory oriented regimes that may arise around the world due to fear of cyber-attacks.

Notwithstanding this consensus in support of the Framework, and its clear record of success, some continue to advocate for imposing cybersecurity solutions upon industry. This would be a mistake. As I noted, these actions would not only prove to be ineffective in addressing cybersecurity but run the risk

of making us less secure by directing critical, limited resources towards issues prioritized by regulators as opposed to allowing companies, who best know their business and information systems, to appropriately respond to the risks they are seeing every day. These actions also undermine the existing public-private partnership model. While we recognize the important role of government, and believe that government assistance is vital to our mission, a regulatory approach will undermine that partnership. Our first and foremost recommendation to the Commission would be to explicitly reject a prescriptive regulatory approach and reinforce that government and industry should continue to work cooperatively, building upon the many different voluntary mechanisms that are already in place today. Examples of this include the Communications sector's ongoing work with DHS, the NIST cybersecurity framework, the NTIA multi-stakeholder process and the recommendations offered by the Communications sector in FCC CSRIC Working Group #4 from 2015.

With that, I would like to address some specific areas that we were asked to cover in our opening statement. We were asked to speak to three specific areas and then provide recommendations to the Commission. Those areas are: first, the biggest challenges we are seeing to critical infrastructure; second, current approaches that we believe are effective; and third, promising research and innovation that may address those challenges. The following are some high level thoughts in each of those areas followed by a set of recommendations for the Commissions consideration.

Biggest challenges in critical infrastructure today and over the upcoming ten years.

- *Complexity.* As the saying goes, complexity is the enemy of security. While previous concepts like Defense in Depth and perimeter defense continue to have merit, the rapid increase in the number of devices and access points make it more difficult to rely upon a perimeter defense model. The attack surface is growing exponentially, and defending against ever-more sophisticated attackers, including nation states, has created an extremely complex environment that makes it difficult to rely upon a perimeter defense model. We believe that companies should operate under the assumption of not "if", but "when", they will be impacted by a cyber-attack. For this reason, the response to an attack, rather than simply prevention, has become a much more critical component of cybersecurity. Further, as discussed above, as increasing layers of virtual and physical networks are leveraged to provide critical services, such as the Internet of Things, simple regulated solutions are insufficient and could actually prove counter-productive. The complexity of the environment supports the continued evolution of the public private partnership model.
- *Increasingly sophisticated adversaries.* While cyber incidents, to the best of our knowledge, continue to leverage predominantly known vulnerabilities, Nation states and other entities are becoming increasingly more sophisticated in their approaches and attack vectors.
- *Convergence.* With the transition to IP-based and software defined networks (SDN) and Network Function Virtualization (NFV) the communications critical infrastructure will become increasingly reliant on critical assets outside its domain. Examples include operating systems, supply chain vendors, and an increasing dependence upon IT.
- *Need for better computing/network architectures*. For large enterprises, the combination of a highly distributed networks and sophisticated, nation-state and criminal actors, makes it very difficult to prevent attacks. Thus, as I noted earlier, a focus on Response and minimizing the damage from an attack have become increasingly more important. As such, we need to move towards newer computing/network architectures that enable a more flexible, adaptive response, leveraging new tools such as virtualization and the cloud.
- *International Governance*. Many cyber threats originate overseas. The complexity of international collaboration, given a wide variety of legal, policy and cultural landscapes, and lack of a coherent strategy gives rise to concerns about confronting the cyber threat on a global scale.

- *Regulatory Creep*. The Communications sector has been encouraged by the recognition among most Federal policy-makers that the best way to bolster our nation's overall cyber defense is through reliance upon voluntary mechanisms rather than compulsory standards or obligations. The inherently backward-looking nature of regulation is ill-suited for the challenges of cybersecurity. Our cyber adversaries are highly sophisticated and adaptive, and it is essential that industry be afforded the necessary flexibility and agility to respond to a constantly-changing threat landscape and to continuous innovation by cyber criminals. Both the NIST Framework and the codification of the NIST process via enactment of the Cybersecurity Enhancement Act of 2014 reflect and advance the clear Federal policy preference for reliance upon voluntary mechanisms and industry-driven initiatives to combat cybersecurity threat. However, as I discussed above, we are concerned that some agencies are retreating from the core policy principle that network security is best achieved through voluntary measures. In addition, there are instances in which agencies appear unaware of the manner in which their regulatory initiatives may conflict with, or adversely effect, cybersecurity related activities supported by Congress and the Administration, such as cyber threat information sharing. We are also concerned that multiple agencies, at multiple levels of government, are becoming more involved in forging cybersecurity policy proposals. The end result is that critical infrastructure owners increasingly face duplicative and conflicting regulatory obligations that do little to materially enhance cybersecurity. Government must partner with industry to ensure that companies establish and maintain an active and agile cyber defense posture, but it must also recognize the limits of prescriptive mandates in this area and guard against regulatory overreach and the imposition of redundant or conflicting rules.

Current approaches that are proving effective in addressing those challenges.

- *NIST Cybersecurity Framework*. The Communications Sector supports the NIST Cybersecurity Framework. The Framework allows for a flexible, risk management model and non-regulatory approach to cyber similar to what I discussed above and is of particular value to enterprise-risk management. We were involved in the Framework from its inception, including participating throughout its development, and have taken efforts to promote it within our sector. Communications Sector executives have appeared at a variety of events, including with one of our major CEOs appearing at the release of the Framework. The Communications Sector has also worked extensively to adapt the Framework to our sector. One highlight of those efforts was our participation in FCC CSRIC Working Group #4 last year, which involved over 100 representatives from across the industry and culminated in the release of an over 400 page report including use cases, among other materials, for how the Framework could be applied across the each of the 5 key portions of the sector.

- *Public private partnership model.* As noted previously, mandates will not only fail to help address the situation, they will substantially hinder efforts given the evolving nature of the threat. As I described in detail earlier in my remarks, the Communications Sector has a long history of working cooperatively and productively with the Federal government, and continues to support that voluntary partnership model. We believe the Commission should make it a point to reinforce that approach in its recommendations to the next Administration.

- *Information sharing legislation*. The Communications Sector also applauds Congress on the passing of vital cybersecurity legislation last December. The Cybersecurity Act of 2015 included the Cybersecurity Information Sharing Act of 2015, which contains important provisions regarding network monitoring, defensive measures, and information sharing. One of the principal challenges that we faced in information sharing was the continued legal uncertainty around cybersecurity itself and information sharing more specifically. In the past there were a myriad of statutes to review prior to electing to share information, which only served to delay the process and prevent the real time sharing of threat intelligence. The recent

legislation is intended to clarify the legal framework around information sharing and the Communications Sector is continuing to evaluate and implement the authorities provided within the legislation. We have formed a CSRIC working group to address information sharing, the CSCC has also formed a strategic information sharing committee, which I currently chair, and we have had DHS and the Department of Justice conduct multiple briefings to both the CSCC and sector attorneys to determine how to proceed. Much of that work is still evolving. Through the combined efforts of DHS and the Department of Justice, in particular the guidance recently issued to implement the legislation, the continued development of the DHS Automated Indicator Sharing (AIS) Portal, and continued efforts within the industry, progress is being made.

Promising research and innovation that may address those challenges in the future

- *More Resilient Computing Architectures (SDN/NFV/Virtualization).* One area that many sector members are focused on is moving towards more distributed architectures where data and security is virtualized in the cloud. This concept allows for security to shift from being a physical appliance to having a security "wrapper" around each instance of various data sets. If there is an attack, the new architecture would make it possible to shift resources around, quarantine data, or limit an attacker's access to resources outside of a specific data set. Thus helping to limit the impact. In effect, the architecture takes a page out of the attacker's playbook to distribute the architecture and enable a more flexible, nimble and resilient response capability.
- *Big Data Analytics (BDA) for security.* NSTAC recently completed a report discussing the use of big data analytics for National Security and Emergency Preparedness. BDA provides potential capabilities to enhance detect and protect functions under the NIST Cybersecurity Framework and response. We recommend the Commission review the BDA recommendations, which describe how government can leverage BDA for these purposes including cybersecurity.
- *Secure Software Development/Software Assurance.* NIST is currently researching tools to better assess or assure secure software development. As networks become more dependent upon software, determining how to promote the use and development of these tools for software developers is becoming increasingly more important.
- *Strong Authentication.* There are also a variety of tools being developed to enhance authentication. The Administration has started discussing this as part of a proposed campaign on the use of 2-factor authentication. Determining how government can better promote stronger authentication in a non- regulatory manner could also benefit security.

Recommendations to propose to the Commission.

- *National Incident Response Plan.* The U.S. government needs to finalize a formal incident response plan that outlines how government will organize itself and work with industry in the event of a large scale cyber disruption. This was a key finding of the recent Cyber Storm exercise conducted this past March. While we understand that the Administration is currently engaged in this activity, it is critical that we have a plan in place before we encounter a large scale attack that may impact critical infrastructure.
- *Eliminate Duplication.* There are currently a wide variety of government initiatives that span a range of agencies. This makes the current process for industry engagement highly inefficient. Also the continued engagement by regulatory agencies undermines the public private partnership process preferred by many in both government and the private sector. More clarity about how government will interface with industry and highlighting that prescriptive regulation will not be effective, and could in fact be a detriment, to better security would both be helpful to enhancing the partnership model with industry. The Commission could partially

accomplish this by reaffirming that the sector specific agencies, as designated by the President, are the appropriate interface with industry.

- *International*. Many cyber threats emerge from overseas, increasing the importance of collaboration among international partners. There remains a need for a more concrete strategy for how to address international collaboration and response, and the effective development of global norms.
- *Domestic preparedness.* Beyond the Federal Government there remain concerns around the level of preparedness among other government entities, and in particular at the state and local level. One possible solution to this challenge is to provide incentives/grants to States to assess their risk, and to take measures to ensure the continuity, both physical and cyber, of the essential services they provide to Citizens within their State. The NASCIO Cyber Disruption Planning Guide and efforts by the National Governor's Association should be supported.
- *NIST Framework.* Continue the focus on the NIST Framework. But instead of expending time and resources drafting "Version 2.0"of the Framework, efforts should be directed to the potential application of the existing Framework in other areas as the attack surface continues to evolve. For example, stakeholders should leverage the Framework to develop use cases for security in the IoT domain. The Department of Commerce, NIST and NTIA can play an important role in bringing together disparate industries with a role in the IoT ecosystem to address these concerns.
- *Encourage new technology/resilient network architectures.* Develop/support strategies for how new technology can be leveraged to improve security. Given the increasing complexities of the cyber environment that is we also need to move forward on strategies for how to evolve computing architectures to be more inherently secure. This can include government leveraging its procurement capabilities in adopting new technologies to spur the market, or other initiatives such as the NIST Cybersecurity Center of Excellence (NCCoE).

In closing, let me once again thank this Commission for their ongoing and important work. We appreciate the opportunity to offer our thoughts on this matter and continue to believe that by working together we can help make the world a safer place.

Dr. Wm. Arthur "Art" Conklin

Good Morning Chairman Donilon, Vice-Chairman Palmisano and Distinguished Members of the Commission, I'm Art Conklin and while I'm here today as an associate professor of your host institution, the University of Houston, the views I'm presenting are my own, and are the product of over two decades of working in cybersecurity. I would like to thank you for this opportunity to address the Commission today.

I am a child of the space race in the 60's and 70's. I built my first computer at age 14, and dreamed of being an astronaut. Although dreams change, I am forever shaped by watching what we as a nation did those many decades ago. What drove us to the moon, and ultimately beyond into today's amazing world of the Internet and the Internet of Things, was people. Educated, talented people, but also people driven by a purpose. My desire to become an astronaut led me to multiple college degrees, with a stint as a Naval Officer sandwiched in the middle. Now, two doctorates later, with all of my technical cyber abilities, I don't see our main challenge as technical, but rather one of a more difficult nature to overcome, a lack of people possessing the skills we need for our future.

Cybersecurity is often viewed as a technical IT thing that requires specific computer skills. And yes, to a degree this has truth. Cybersecurity does have a lot of technical issues, and it does involve computers. With the rapid move to connect our IT systems to our critical infrastructure elements, these systems are more than just your office PC or server. One of the fundamental challenges we face every day in cybersecurity is that security was not designed in from the beginning, and as a result we have had to bolt on solutions afterwards – like changing parts on your car as you drive down the highway.

The foundation behind everything we build, everything we deploy, and everything we use, is people. People create new technology, and one doesn't have to listen hard to hear the siren call that every industry needs more technically skilled people. But the problem is more complex than just a simple shortage, the issues run deeper than that. Yes, we need more skilled cybersecurity engineers, more secure programmers, more technicians, firewall people, investigators, . . . the list goes on, but this is the easy part. But what about the line of business manager and the project manager? The VP of development, of R&D, of Marketing? These are the people that are currently creating the next generation of things. Things that specialists will have to go figure out how to secure in the future. Either we address security at this point in the value creation cycle, or we forever continue fire-fighting and bolting on security after the fact. These people need to learn about the risks and values of security. The entire value chain of technology creation plays a role and needs to learn from our problems and failures. Yet, for many of these positions and the people in them, they don't even know they need to know what they don't know - Rumsfeld's unknown-unknown.

The Internet was designed without any conceptualization of making it secure, and it has become problematic now that our lives depend upon it. Now we are designing the Internet of Things right, and in the same vein – get product out the door, be the first, worry about security later. We shall surely repeat the history that we did not learn with the Internet. When we look at critical infrastructures, pipelines, the electric grid, refineries, manufacturing, even our large building automation systems controlling HVAC and energy usage – they all have a common denominator; Computer controls. And these controls are being interconnected to business networks, and the Internet, at the speed of 21st century technology change. Yet the entire industry that designs and builds our critical infrastructure, SCADA systems and the like, still treat security like it's the mid 1990's – they have heard about it, talk about it, but are far from really addressing it. Our future is being driven by well-meaning people without the skills or understanding of the need to build a safe, secure future, from the beginning.

President Kennedy charged the nation "I believe that this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to the earth." That little detail of returning safely made the whole venture much more challenging technically, but also necessary for it to have any lasting purpose. We need a similar rallying directive for the future of

our technology driven society – we need to make it safe and secure, from the beginning, from design – before we create another Internet, useful, but hard to maintain and problematic in living up to all our dreams and aspirations.

To directly address the people problem, we need to advance widespread education on the role of security in technology. I am not suggesting we make everyone a technical expert. Far from that, instead we need to craft the correct lessons for the correct jobs. We need to create education efforts that addresses the wider range of impact of security and risk in our advancing technological based society. From K – 12 onwards, we have people using technology, we owe it to them and our society to help everyone understand the roles technology and security play hand in hand. In the oil and gas industry – safety is at the heart of everything they do. Don't believe it? Walk into an Oil and Gas company headquarters while using your smart phone. Or walk up and down stairs without using a handrail. You will get the point quickly. It is part of their DNA, a core value – for everyone in and out of the firm. Technology is part of our nation's DNA going forward, and we need to have a responsible approach to understanding and managing the risks and rewards of creating, building and using the technology that will power our future. Understanding that technology brings reward, but also risk and understanding each and everyone's role in managing the risk needs to become a core value. This is not the economy or the world of the last century. This requires an investment in education, an investment to drive the changes we need in our systems, how we buy them, design, create, build and operate them. If we allow industry to completely lead the charge, they will continue down the path they are on, for it optimizes benefits for them, not necessarily those of society. Do we want robots or cars with the same software trustworthiness that we have lived with for the last few decades?

There is some good news on this front. We have several major programs involving cybersecurity education. The first is the Scholarship for Service, an NSF backed program that is designed and is delivering technical professionals into government service. Another is the NSA and DHS Centers of Academic Excellence in Cyber Defense Education program, a program that sets standards for academic institutions of higher education in an attempt to create more cybersecurity graduates across many fields. The last is the National Initiative for Cybersecurity Education, a NIST executed coordination effort designed to assist in the alignment of cybersecurity education from K to PhD across federal and eventually industry workforce needs.

The bad news is these programs are all focused primarily on the IT technical space of the problem, not the broader spectrum of additional jobs that have cyber security responsibilities. Each is also constrained to support only specific items, not a lot of variety. We will need people with cybersecurity understanding in medicine, law, treaties, policies, criminal justice, engineering, and virtually every field. Each of these will be different, they may have the same foundations, but the security lessons will be integrated into their primary discipline. This is more than just an IT problem. While many may think IT technical people will help secure our critical infrastructures, there are wide swaths where we use operational technology (OT) systems and these are different and not really compatible with IT security. So even on the technical front, we currently go wanting for professionals and trained people.

To make a change in direction for the future, we need to set a new course.

First, we need a charge, from the top. Much as President Kennedy did with the space agenda. Technology is this generation's space race, and we need the guiding leadership imperative to tell us to do it securely and safely. Security and risk need to be part of every system design and solution, not bolted on later as failures show need.

Second, we need to dramatically expand the scope of education with respect to making people technology ready. From Kindergarten onwards people are using technology. Everyone needs to learn the role of technology and risk, so that they can do their part with intelligence. The next generation needs to learn the lessons we have learned before about building reliable systems, safe systems and systems. We are counting on them for our infrastructure needs of the future, we want a safe, reliable and secure future. We need to rethink the field of cybersecurity and risk management education and

integrate it into a wide spectrum of disciplines. We need to end the days of program managers, marketers, management and finance putting security and risk responsibilities into the hands of those outside the value creation chain. It has worked to get us this far, but it is failing to keep pace and we are gambling with our own infrastructure. Does anyone want the wireless enabled pacemaker that security was considered "too much trouble to integrate in, and the risk is minimal"? Besides, if it becomes a problem we can patch it later.

Expanding cybersecurity education can be done through the existing programs, but not at their current funding or chartered levels. We need to expand them all, increase the breadth of our talent improvement across a wide range of fields. From political science, to biology, to engineering, to business, to sociology; technology is our future and its history will be marked by the levels of risk and security it experiences. We need to open up funding to help local schools, where the education happens. We need the equivalent of block grants to drive the changes from the ground up, driven by local need.

We need to expand the resources from middle school to PhD in the area of STEM education. This is our future seed corn, and educating them for the future rather than about the past is our challenge. One of the challenges that one finds is there is a shortage of teachers and equipment to do this. If someone has reasonable cybersecurity skills, why become a teacher, when you can make significantly more in industry. My wife reminds me of that now and then. We need to address the skilled teacher shortage in cybersecurity.

The advancement of technology means advancement in skills and labs are also needed. In the industry this is called capacity building – and it is a real shortfall, for schools do not have the budgets to create and maintain these programs. Most successful programs have a research component and the education side gets the leftovers from the research. This limits access and capacity significantly. Currently there are slightly over 200 schools designated as Centers of Academic Excellence in Cyber Defense Education. At present, this designation carries no financial incentive and schools have dropped out of the program because of costs of maintaining a program.

There are a lot of current funding sources for cyber security, but they are all aimed at solving a specific problem. Grants for one purpose or another, but for the development of specific solutions to specific problems. Not in any consistent significant manner towards the cost of cyber security education. Assume 300 schools, if one funds each school only $100,000 a year, this makes the investment $30 million. And make this money open for each school to decide how to spend it – let local decisions create multiple local optimums, raising the water level where it needs to go up and will do the most good, rather than trying to raise the whole ocean. Yes, this not small money, but in the scope of what the return on that investment – huge. To expand the program into other areas, increase the money – put something like $20 million into the program offices (NSA and NIST NICE) to expand programs, and watch the investment bear fruit. The challenge in DC is never the amount of money, but in whose budget does the line go. Cyber security education crosses all disciplines, but the best bet is one that is already winning, and for this I would suggest looking at the Centers of Academic Excellence program run out of the NSA – they have a nearly 20 year track record of doing wonders with little resources, imagine a world where they had a solid line item and authority to back it for years.

I know everyone always asks for money, or for special items associated with their view of security. And I am as well, for we have a resource shortage in education at all levels that is limiting our ability to create the people we need. But I am also asking that the issue of cybersecurity and critical infrastructure be viewed in a larger context – as part of our technological fabric that we are building the future of our society. I am asking for a leadership statement that provides the motivation to go to the moon and back. I am asking the panel to recognize that the underlying issues of security are wider spread than just being an IT technical issue. We need to address the missing skills and lost opportunities before we create the next technological problem child. People have always been our best asset and this is one area where government intervention can improve all aspects of the future. We

don't need free fish, we need to learn how to fish. Teach the masses to fish and we shall all eat well for a long time to come.

I look forward to answering any questions you may have.

Marty Edwards

Chairman Donilon, Vice Chairman Palmisano, and members of the Commission, my name is Marty Edwards, and I am the Director of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) within the National Cybersecurity and Communications Integration Center (NCCIC) at the U.S. Department of Homeland Security (DHS).

The NCCIC was established to serve as the central government interface to coordinate cybersecurity and communications matters between all federal departments and agencies; state, local, tribal, and territorial governments; the private sector; Information Sharing and Analysis Centers (ISACs); critical infrastructure owners and operators as well as international entities.

Thank you for the opportunity to speak with you, and contribute to your important efforts to improve the cybersecurity resilience of our Nation.

Deputy Assistant Secretary for Infrastructure Protection Bob Kolasky has provided you with an overview of how the Department leads and executes our role in securing critical infrastructure – from the continuously evolving threats in both the physical and cyber domains.

My remarks will focus on the often misunderstood computerized systems that silently operate the majority of our critical infrastructure – so called Industrial Control Systems (ICS) – and our increasing reliance and dependence on the continuous and safe operation of these often neglected networks. I will also share some thoughts on evolving cybersecurity challenges associated with the "internet of things" and other embedded systems.

Industrial Control Systems (ICS) have been around for many years, and for the most part have remained as very specialized computing environments designed for the safe and reliable operation of industrialized processes such as energy production, transmission and distribution; chemical plants; water and wastewater treatment plants and systems; food and beverage manufacturing; transportation systems; etc. These systems were originally intended to be operated in isolation from other networks and systems – and in many cases were the 'first computers' to be introduced into industry. These legacy installations can have a life expectancy counted in decades – a compounding factor when you consider the speed of technology advancement and the continuously evolving cybersecurity threat landscape.

Growing demands for increased data about plant and process efficiencies, and trends for more remote monitoring, operation and engineering capabilities in these facilities have caused these "islands of automation" to be interconnected – first to corporate network environments – and now in many cases – directly to the internet, which further exposes the 'soft underbelly' of these legacy systems and installations to the threats and risks of operating in today's cyber ecosystem. These systems were never designed with security built in, and now we are attempting at the last moment to bolt security on – with limited success.

From information gathered through services such as our cybersecurity risk assessments and incident response activities, we can clearly see that both government critical infrastructure systems, as well as private sector systems – are continuously challenged to keep up with the ever changing demands placed on them from a cybersecurity perspective. Whether it is a misunderstanding or incomplete knowledge of the risks and threats posed to these systems, or a lack of financial resources to protect these systems – it is my opinion that our combined defensive position is lagging behind current adversarial offensive capabilities.

We must continue to invest proactively in outreach and awareness programs specifically aimed at the owners and operators of these critical systems – to educate them on the evolving nature of the cyber threat, and how to economically protect themselves in this complex environment. It is not always about technology, and I would recommend that governments and companies alike must invest in human capital first, sound policy and procedure second and thirdly with appropriate technology being identified by the capable people that have been put in place to protect the systems.

Organizations such as the NCCIC have had profound success in sharing actionable information to organizations to better enable them to protect their networks and systems – but we could have a significantly better perspective on the true health of the cybersecurity ecosystem with an increase in voluntarily submitted information such as reports on cybersecurity incidents. It is only through the correlation of data voluntarily submitted from the private sector with other data such as law enforcement and intelligence information that allows us to continue to improve the quality and applicability of the information that we produce. Such information sharing initiatives must also be scalable in order that industry and government alike can commit the resources required to keep pace with the evolution of the threats – we cannot do this alone, and we are in this together with neither government nor industry uniquely holding every piece to the puzzle.

My ICS-CERT team, which focuses on systems such as Industrial Control Systems, medical devices, automobiles and other embedded systems that don't fit the typical enterprise system mold, offers many products and services to help both government and private sector owners and operators of these systems harden and protect them against attacks. A few highlights are:

- Focused risk assessments. We deploy teams into the field at the request of stakeholders and systematically evaluate the cybersecurity of their infrastructure systems and networks, providing them with specific recommendations on where to improve their cybersecurity posture. Utilizing the Cyber Security Evaluation Tool (CSET™) that we developed, owners and operators can also perform their own self-paced assessment.
- Correlating data provided by the intelligence community, law enforcement or data that the private sector has voluntarily submitted ICS-CERT can identify trends and campaigns such as the BlackEnergy series of malware and intrusions. If required, we can send incident asset response teams to the field with advanced forensics tools and equipment in order to identify the problem and quickly return the infrastructure to normal operations. These incident response teams are focused on mitigating the effects of a compromise – working hand in hand with our law enforcement partners who are focused on threat actor attribution and criminal prosecution. In the case of significant intrusion campaigns like BlackEnergy we have shared our analysis with our partners by providing unclassified and/or classified briefings at multiple cities around the country.
- Many of our products and services are provided in order to shape the cybersecurity ecosystem and promulgate best practices. Whether in the form of newsletters, alerts and advisories or technical white papers – we strive to communicate trends in cybersecurity of these complex systems, and alert our constituents of any weakness, vulnerability or problem that they need to be aware of. We have provided classroom based cybersecurity training to over 10,000 security practitioners and countless others through our web-based courseware.

Further compounding these challenges in the industrial critical infrastructure area, is the continuous evolution of what we are now calling "the internet of things."

Our day to day lives are quickly becoming interconnected with absolutely everything around us. A consumer can link their smart phone or tablet with devices intended to provide us with unimaginable access to data on every aspect of our lives. We can remotely change the temperature of the air conditioner in our home or of the oven that is cooking the roast beef for dinner. Our automobiles link to our devices in order to play the latest songs or to tell us when we need the oil changed. Implantable medical devices such as insulin pumps, pacemakers and the like are able to provide us vital data on their performance, our health and can even be managed by our health care provider.

This connectivity brings incredible benefits to consumer and society as a whole – but I fear that we are adopting technology at an unsustainable rate, often without any regard or concern to the increased risk that this interconnectivity can bring.

It is one thing to imagine someone maliciously playing a prank on us by turning the lights on and off in our homes – it is something completely different to think of the ramifications of someone changing the dosage of insulin being provided to a diabetic.

Initiatives must be explored and developed to educate the general consumer about the risks of connecting 'everything to everything' and standards must be developed in simple plain language to enable consumers to tell whether or not a product has 'good cybersecurity' or 'bad cybersecurity'. These initiatives will not be easy or simple, and require significant systematic and strategic investment by both governments and the private sector. We must get to the point where manufacturers of all devices are held accountable for the cybersecurity of their devices – in accordance with rational risk assessment methods and the intended use of the product. Products with life safety implications must have more stringent controls than those intended for entertainment applications – but this too is complex when these devices are operating in an interconnected environment where an entertainment device with poor security could impact the operation of a life safety device with unintended consequences.

We can overcome these challenges through systematic improvements in education and programs at all levels to cultivate an environment where manufacturers and consumers alike become knowledgeable on cybersecurity matters and through continuous investment by governments and private entities in this area.

Thank you Mr. Chairman and the committee for inviting me to provide input into this critical process, and the Department stands ready to assist in any way that we are able.

Major General Reynold N. Hoover

Chairman Donilon and members of the Commission, on behalf of my boss, General Frank Grass - the Chief of National Guard Bureau - thank you for the opportunity to appear before your Critical Infrastructure session to highlight the National Guard's capabilities in the cyber domain. My name is Major General Reynold Hoover, the Director of Intelligence and the Director of Command, Control and Computers on the National Guard Bureau staff. It is a great pleasure to be here today to address cyber security issues impacting the world in which we live, do business, govern, and defend our Nation. But more importantly, to highlight for you how the National Guard is positioned today, and in the future, to protect America's cyber critical infrastructure.

The challenge of protecting the cyber domain is a team sport, and one in which we believe the National Guard is uniquely qualified and positioned to support and partner with both Department of Defense and non-Department entities, and including the private sector. Our commitment to cyber defense partnerships becomes more and more important every day as we, as a society, become more interconnected and dependent upon online systems. As our level of connectedness increases, the amount of targets and opportunities for our adversaries grows at the same pace. Indeed, the roll-call of government entities, trans-national corporations, small business, and private citizens who have been victims of a cyber-attack grows by the hour.

The rapid advance of technology that continues to bring convenience and networking to our fingertips and into our homes, our government organizations and our businesses has also brought the specter of identity theft, cybercrimes, foreign government and industrial espionage, and critical infrastructure attacks that pose tremendous threats to our communities. The speed and pace 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 interests in cyberspace defense and critical infrastructure protection; and, I know I speak for the more than 400,000 women and men of the National Guard who are serving around the world when I say we are always ready, always there.

As the Commission looks to build a path for continued progress into the future, I would like to take a moment today to highlight the National Guard's important role in building, maintaining, and growing enduring partnerships. Working together, the National Guard, state, federal and private sector partnerships can help prevent and disrupt threats to our collective digital infrastructure. Whole of nation strategy – a partnership at the local, state, tribal and federal levels; and, a partnership with the private sector. All committed to working together to safeguard our economic and national security.

The National Guard in the 54 States, Territories and the District of Columbia in the Army and Air Force are no strangers to defending the homeland and partnerships. When disaster strikes, State Governors across the country call upon the National Guard to bring relief. And, because your hometown Guardsmen are close at hand, they are our community's and our nation's first military responders.

The National Guard's role in defensive cyber operations can be traced back to preparations for the Y2K bug in 1999. At that time we established 54 Computer Defense Network Teams to help prepare for anticipated coding problems associated with the start of the new millennium. State Governors were given the authority to command these National Guard cyberspace forces just like other National Guard capabilities when in a state status. These teams have stayed in existence and remain a force that brings a capability to support domestic missions. By 2019, the NG will grow our cyber capacity numbering in excess of 2,800 personnel across 34 states beyond the level of these existing Computer Network Defense Teams and have re-designated these teams as Defensive Cyberspace Operations Elements.

The National Guard will build this skilled cyber workforce trained to the Joint Standard.

Today, the National Guard is active in nearly all facets of cyberspace operations. We are aligned with the proper authorities to support decision makers at all levels including State Governors, Active Duty services, and with their various Commands. Our Guardsmen and women are in every State and

Territory. Because of this, we are able to develop personal relationships with our neighbors, friends and colleagues. This allows the National Guard to support cyberspace operations in careful collaboration with other U.S. government departments and agencies, including the Departments of Homeland Security, Justice and the Intelligence Community.

We have units that are performing federal Title 10, Active Duty missions in support of both the Army and Air Force as well as U.S. CYBER COMMAND. At the state-level National Guard personnel can be utilized under the National Guard's Title 32 authority or in a State Active Duty status under the Governor's direction.

As part of a layered defense, today's National Guard provides a critical defensive cyber capability available to 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-governmental entities was recently strengthened by the Deputy Security of Defense who signed an interim policy guidance that outlines how the National Guard can Coordinate, Train, Advise and Assist cyber support and services to organizations outside of the Department of Defense.

This new guidance allows our cyber warriors serving in a National Guard Title 32 capacity to consult with entities outside of the Department of Defense in order to protect DoD assets, enhance situational awareness, provide for DoD mission assurance requirements and ensure cybersecurity unity of effort.

Governors of course retain the authority to activate their National Guard in a State Active Duty status to respond to a cyber incident or other disaster, in accordance with state law. We frequently exercise these capabilities in order to ensure we are prepared. These exercises range from the local to National level and offer another tremendous opportunity to better familiarize ourselves with private sector and other governmental capabilities, personnel, and key cyber terrain in order to enable rapid response when it's time to "Call out the Guard".

Let me just highlight a few of those exercises:

- Cyber Buckeye, at the state level, provided National Guard leaders an opportunity to assess the Ohio National Guard's depth of understanding and operational competency in managing cyber incidents.
- Cyber Yankee, a regional level exercise that engaged cyber operators from across FEMA Region I, this exercise focused on the implications of an event that cascaded beyond state boundaries, ultimately involving all six states within the FEMA Region.
- Cyber Guard, a national level exercise hosted by USCYBERCOM provided a "Whole of Nation" training exercise on responding rapidly to a domestic cyber-attack causing a catastrophic natural or man-made cyberspace disruption. The exercise also provided an opportunity for the National Guard to train with industry partners, our active component colleagues, and all of the relevant federal agencies.
- Finally, Cyber Shield, the National Guard's premier unclassified collective training event, provides an assessment of Defensive Cyber Operations-Element in a defensively focused cyber exercise environment designed to engage our joint service and state partners.

As might be evident from our cyber training and exercises, partnerships are a key component of what we do.

So just who are the National Guard's cyber warriors?

They are women and men, trained to the same standards as their 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 and 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 appropriate authority. And, they are intended to set conditions for other response elements as the situation requires.

They are soldiers and airmen living in your communities who are committed to protecting America's interests 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 the dual use capability to operate in a State Active Duty status. The first three teams are being activated in 2017, four more will activate in 2018 and the last three will activate 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 Cyberspace Operations Elements across the country.

Our Air National Guard also plays an important, and integral part in DoD's defense-in-depth strategy, they will have 12 Cyberspace Operations Squadrons geographically dispersed around the country comprised of 71 airmen each by the end of Fiscal Year 2018. The Air National Guard has already began supporting the Air Force by providing operational rotations.

So what does all of that mean in terms of posturing for future cyber and critical infrastructure threats?

It means, the National Guard is committed to partnerships in 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, the National Guard's cyber warriors are currently involved in and building greater depth in infrastructure protection, and many other types of cyberspace operations, in support of U.S. Cyber Command.

And, it means, that the National Guard is there to provide critical cyber capabilities to the 54 States, Territories and the District of Columbia in support of the Department of Defense, Federal and State responses as part of a layered, and partnered, defense. More importantly, perhaps, it means our National Guard cyber assets may be shared by the states and across state lines through pre-arranged mutual assistance partnership agreements known as Emergency Management Assistance Compacts or EMACs – this is just another way the National Guard partners to deliver capability when it is needed, where it's needed.

Let me close here by saying, I believe that we, in the National Guard, are laser focused on defending the nation in cyberspace from foreign and domestic adversaries who wish to exploit, disrupt or destroy critical public and government infrastructure and in building the enduring partnerships to do this effectively.

As a traditional drilling Guardsmen I am deeply honored to be a part of the National Guard's cyber effort and to be here with you today.

Thank you and I will be pleased to answer any questions you may have.

Robert "Bob" Kolasky

Good morning Chairman Donilon, Vice Chairman Palmisano, and members of the Commission. I am Bob Kolasky, the Deputy Assistant Secretary for Infrastructure Protection within the National Protection and Programs Directorate (NPPD) at DHS. I am grateful for the opportunity to participate in this important hearing about enhancing our national cybersecurity. NPPD serves as the de facto cyber and infrastructure protection agency for DHS – in fact Congress has proposed legislation to rename the Directorate as such – and in that role is responsible for enhancing the security and resilience of the Nation's critical infrastructure against all hazards, including cyber threats, and providing Federal facility and network security.

Since its establishment, DHS has played a lead role in critical infrastructure protection. Initially the Department's focus was working to secure critical infrastructure toward terrorist attacks – an issue that remains a priority – but the mission has subsequently evolved to include both physical and cyber threats. The legal authorities we have in place to include the Critical Infrastructure Partnership Advisory Council structure as well as the Protected Critical Infrastructure Information authority have enabled us to work effectively to mitigate risks to the Nation's security.

My remarks today focus on the general approach that the U.S. Government has taken to critical infrastructure security and resilience (CISR) as well as the specific steps we have taken, working with the critical infrastructure community, to raise the level of cyber security across the 16 critical infrastructure sectors.

PPD 21, EO 13636 and CISR

Issued on February 12, 2013, Presidential Policy Directive 21 established national policy for critical infrastructure security and resilience. PPD 21 delineates 16 critical infrastructure sectors, defines the need for an integrated physical-cyber approach to risk management, emphasizes the importance of public-private partnerships, expands the mandate for information sharing, establishes the need for critical infrastructure situational awareness and calls for additional research and development efforts. In addition, PPD 21 defines agency roles and responsibilities for critical infrastructure security and resilience including establishing assigning the Secretary of Homeland Security the responsibility to "provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure." DHS is also named as the Sector Specific Agency for all or parts of 10 critical infrastructure sectors, including the Communications and Information Technology sectors.

PPD 21 was issued on the same day as Executive Order 13636 on Critical Infrastructure Cyber Security and those two policies were implemented in an integrated manner. On behalf of the DHS Secretary, I led the Department's implementation of both policies as well as the interagency Integrated Task Force which included representatives from across the Federal government, as well as State, Local, Tribal and Territorial governments, the private sector, and non-governmental organizations. Among the accomplishments the Task Force achieved was a review of the public-private partnership model for critical infrastructure, identification of critical infrastructure where a cyber security incident could cause catastrophic consequences (the "Section 9 list"), identification of possible incentives for enhanced cyber security, enhanced practices for cyber and physical situational awareness, and development of the National Infrastructure Protection Plan. We also worked closely with NIST and industry on the development of the Cyber Security Framework.

Where we stand today

Two years after the Task Force disbanded, it is my view that the Nation has been well-served by those presidential policies and we have seen major enhancements in the level of, and attention to, cyber security across the critical infrastructure community. For example:

- The information sharing environment has been greatly enhanced, to include improvements in automated information sharing. Based on recently passed legislation, the National

Cybersecurity and Communications Integration Center (the NCCIC) serves as the hub for critical infrastructure information sharing and has developed mechanisms for automated information sharing of cyber threats indicators with critical infrastructure organizations; based in part on the President's Executive Order of 2014, Information Sharing Analysis Organizations continue to develop to connect to the NCCIC and to promote public-private and private-private information sharing; and DHS and other sector specific agencies have partnered with the IC to build programs to enable sharing of classified and non-classified cyber information with operators to allow for real-time cyber threat mitigation, including Enhanced Cyber Security Services.

- The NIST Cybersecurity Framework effectively serves as a common risk management approach for critical infrastructure. For example, the great majority of the 16 critical infrastructure sectors have published sector-specific implementation guidance on utilizing the Cyber Security Framework; the Framework is increasingly being utilized as a basis for an expanding cyber insurance market; and, regulating agencies are harmonizing their regulatory approaches with the NIST Framework.
- The strengthened Sector Coordinating structure has allowed renewed focus on cyber security as a national security and business imperative. For example, the Electric Sector has elevated its coordinating council to a CEO-level and is focused on cyber resilience amongst other priorities; the Transportation Sector is piloting an approach to utilize the NIST Framework and intelligence data to prioritize mitigation needs; the Nuclear Sector is working on a joint U.K.-U.S Cyber security exercise in November. And, 12 other sectors have published Sector Specific Plans which discuss cyber security priorities for their sector as part of an overall risk management approach.

Our Lines of Business

Specific to DHS, we have four lines of business by which we help the private sector strengthen its cyber risk management.

1. Our first line of business is information sharing. We share cyber information with our private sector partners person-to-person, via bulletins, and machine to machine. As an example of our person-to-person information sharing, we have private sector companies and groups who sit on our watch floor, and we hold events where we bring together analysts to learn from each other. In addition, we distribute numerous bulletins and alerts that are customers read to learn about threats, vulnerabilities, and ways to protect themselves. As part of that work, we have for years directly and with our grantee CERT/CC coordinated the disclosure of software vulnerabilities. And finally, we have launched our machine-to-machine indicator sharing program, as required by the Cybersecurity Act of 2015.
2. Our second line of business is to help develop and promulgate best practices. We advocate for the adoption of the NIST Framework. We do that in part through workshops, webinars, and other events where we help businesses-particularly small and medium businesses—understand the Framework. We also do risk assessments for companies to help them understand their current risk. These risk assessments range from questionnaires to actual technical penetration tests. Finally, we have a nascent effort to educate Boards of Directors, General Counsels, and other corporate leaders so that they support the work of their internal information risk management team.
3. Our third line of business is incident response. In the real world, you want both the police and firefighters to respond to an arson. Major cyber incidents are similar: DHS and law enforcement both have a role to play. DHS responds to incidents to help the victim find the adversary on their networks, identify the impact—what has the adversary done—and kick the adversary off the network. We are almost always onsite with our partners in law enforcement,

who seek to identify and bring to justice the adversary. But our focus is on the victim and restoring service as soon as possible.

4. Finally, our fourth line of business is broader. It is our work to shape the entire cyber ecosystem. That ranges from our work to stimulate the insurance industry, to our work to encourage companies to build security into their software in the first place, to our work to increase the number of cybersecurity professionals in the nation. We do much of this work in collaboration with other agencies, including the National Science Foundation, the National Security Agency, and NIST.

These four lines of business are how we seek to reduce the national risk by improving critical infrastructure and private sector cybersecurity. We have an additional line of business with respect to federal cybersecurity.

Challenges Ahead

Our current approach to critical infrastructure security has reaped many benefits. From my perspective, however, there are still opportunities to raise the level of critical infrastructure cyber security in the face of the threat environment that we face and

I appreciate the challenge facing the Commission as it formulates its recommendations. Amongst the priority areas that I would offer for consideration:

- Improved assessment of cyber risk and the value of cyber security for the purpose of enhanced national security, corporate, and regulatory decision making;
- Enhanced risk management for cyber-physical systems to include designed in resilience;
- Improved coordination between cyber security, homeland security, and emergency response communities to develop plans to minimize impact of cyber attacks;
- New solutions for government and industry to more flexibly work together to share information and innovate in the face of emerging risks; and
- Scalable solutions for cyber security that can be implemented in resource constrained environments, including by small and medium sized business which serve as suppliers to critical infrastructure.

To conclude, the structures and processes that have been put in place have, in my opinion, enhanced the cyber security to the Nation's critical infrastructure. These structures only work, however, with the investment of time and energy on the government's side to make them worthwhile to industry, the consistent and improved ability to share multidirectional information, the legal protections that enable collaboration and, most of all, trust that government and industry can collaborate to solve problems.

Thank you again Mr. Chairman for allowing me to provide this input into this important process and the Department remains committed to assisting further as needed. I'm happy to answer any questions you or the other members may have at this time.

David LaPlante

In 2013 the City of Houston undertook a project to establish a Cybersecurity Framework (Framework) that would provide a common language for expressing, understanding, and managing cybersecurity risk, both internally and externally. The Framework will be used to help identify and prioritize actions for reducing risk and is a tool for aligning policy, business, and technological approaches to managing that risk. The Framework selected was the NIST CyberSecurity Framework.

As part of the implementation strategy, the City applied for Urban Area Security Initiative (UASI) funding with a two-fold purpose. The first was to provide the needed resources to implement the Framework at the City of Houston. The second was to provide resources to take the lessons learned, plans, templates and other generated resources and create a resource for other municipal organizations in the Houston UASI Region to use as a tool for implementing a CyberSecurity program in their organizations.

In the upcoming testimony, the City will provide more detail around the project and how the resources have been able to be leveraged by numerous organizations as we try to make the region more secure.

Steve Mustard

Mr. Chairman, Vice Chairman and Distinguished Members of the Commission:

The Automation Federation is a global umbrella 501c3 organization of seventeen member organizations and six working groups engaged in automation-related activities. The Automation Federation enables its members to more effectively fulfill their missions, advance the science and engineering of automation technologies and applications, and develop the workforce needed to capitalize on the benefits of automation. The Automation Federation is the "Voice of Automation."

I am the Chair of the Automation Federation Cybersecurity Committee. I am a Subject Matter Expert in automation with an emphasis in Industrial Control System Cybersecurity. In the course of my work, I regularly visit critical infrastructure facilities all around the world, in oil & gas, water & wastewater, chemical, transport, and food & beverage. My comments are based upon observations I've made during these visits.

The cybersecurity threat to the nation's critical infrastructure is significant and we must take action if we are to avoid a major incident that could involve loss of life, damage to the environment, or serious economic consequences. It is well understood that critical infrastructure is monitored and controlled by systems that are very often based on obsolete technology where conventional IT cybersecurity controls are difficult to apply. Critical infrastructure systems run 24/7/365 and it can be months or even years before they can be taken out of service for updates, leaving them vulnerable to a wealth of threats.

Although this is well understood, there remains very limited availability of competent persons who are able to correctly manage the cybersecurity of these systems. Many come from an IT background with little appreciation or knowledge of the key differences between Information Technology and Operational Technology, in particular the emphasis on availability in OT systems as opposed to confidentiality in IT systems. As a result, in many cases, critical infrastructure cybersecurity is limited to management of perimeter security without adequately addressing access control, use of portable devices, backup and recovery, and incident response.

Complacency is the biggest challenge to successful industrial cybersecurity management. Too often, management of critical infrastructure organizations do not take the cybersecurity threat seriously. Most believe that the asset integrity barrier model, consisting of multiple independent failsafe mechanisms such as pressure release valves and shutdown systems, will prevent a cybersecurity incident ever causing an industrial accident. Sadly, every industrial accident in history has been a result of a simultaneous failure of poorly maintained or disabled multiple protection mechanisms.

As security technology has improved, and its deployment widened, people-oriented threats have increased. Social engineering methods are now the dominant primary attack vector. Despite widespread reporting of the risks of social engineering, people continue to succumb to the invitation to click links and download attachments.

Technology is only one third of the cybersecurity challenge. Process and people are the other two, and these are what can make the biggest difference between an incident and a near miss. While technology does need to be addressed, much more effort needs to go into process and people issues. Unfortunately, most cybersecurity management budgets are heavily biased towards technology with little or no attempt to address process and people.

The industrial sector already has a well-proven strategy for managing safety, and this must be applied to cybersecurity if we are to avoid a major industrial accident. At present, this is not the case in many facilities. For example, in any industrial facility a worker will be stopped and reported for not using a handrail while walking up a stair or for not wearing the correct Personal Protective Equipment. Yet there will likely be no such intervention if the same worker is about to plug in an un-scanned drive into a control system workstation.

The Industrial sector also has established and proven safe methods for managing change and yet these are usually not correctly applied to industrial control systems. The result is that changes are made without adequate testing, backups of configuration and program files are not taken, and there is a lack of change records that could be used to identify future issues.

Incident response planning and preparation is also well established but very few critical infrastructure organizations have an incident response plan that includes cybersecurity incidents. While it is common to have drills to verify that incident response plans will work as expected, few of these drills, if any, involve a response to a cybersecurity incident.

Even when a cybersecurity near miss occurs, system custodians, users and even many experts dismiss them, typically because no major incident occurred. Conversely, when a safety near miss occurs, the same people take the event very seriously, reviewing the incident to determine root cause and identifying additional mitigations that can be adopted. Cybersecurity management must change to adopt the safety culture if we are to deal with the risk of cybersecurity-driven accidents.

A good understanding of the provenance of system components is essential to managing system risk and developing mitigations. The trend is to build components from existing libraries and products and this makes provenance a major risk.

There are many excellent resources available to help critical infrastructure organizations improve their security posture. The Cybersecurity Framework provides a starting point for organizations to map out what they should be doing and compare that against what they are doing. The ISA/IEC62443 standard is an international standard for cybersecurity of industrial control systems. Developed by a committee of over 500 subject matter experts from all critical infrastructure sectors, the standard provides clear, voluntary direction, without mandating prescriptive solutions. Like the Cybersecurity Framework, the ISA/IEC62443 recommends a risk-based approach to implementing a cybersecurity management program. This allows for organizations of varying size and risk to apply only the controls that are appropriate to them. Adoption of the standard varies from sector to sector, but where it is applied, for instance in the oil & gas sector, the resulting security posture is significantly improved. Regulations, such as NERC CIP, are also valuable as a tool to improve security posture by enforcing mandatory implementation of security controls. However, in some instances, compliance with regulations becomes a checklist exercise and this approach does not deliver good cybersecurity management.

I recommend a number of actions to address these concerns, as follows:

- A major effort needs to be made change the perception of the threat of cybersecurity and to deliver education in the basics of good cyber-hygiene. This must start as soon as children begin using computers at school and must continue throughout education and employment.
- Cybersecurity skills must become part of standard competency frameworks for industrial employees. The USDOL Automation Competency Model and the Cybersecurity Industry Model can be used as inputs to such activities.
- Specialist industrial control system cybersecurity training is required to bring stakeholders up to the necessary skill level. Such training should be against the relevant standards, in particular the Cybersecurity Framework and ISA/IEC62443.
- More competent industrial control system specialists are required to guide others in the required technology, process and people solutions. Certificate programs based on ISA/IEC62443 ensure that these specialists have the necessary skills to perform the role to the required standard.
- Continued efforts are required to ensure that the Cybersecurity Framework together with the industrial control system security standard ISA/IEC62443 receive broad adoption.

- There must be an increased drive to have products certified to ISA/IEC62443 by ISASecure compliant third parties. Demand from users for certified products will drive vendors to follow the process and this will significantly reduce risk.

If we can ensure that critical infrastructure organizations treat cybersecurity as a potential safety risk and ensure that the cybersecurity near miss concept is adopted across all critical sectors we will have made a major step forward in the fight against the cybersecurity threat.

Scott Robichaux

Thank you to the Commission and for your interest in oil and natural gas. I'm Scott Robichaux and I manage the ExxonMobil Information Technology Cyber Security Center of Expertise. My team is composed of information security experts around the globe, responsible for Incident Management, Investigation, Threat Intelligence, User Awareness and Vulnerability Testing regarding Cybersecurity across the IT environment.

I think it would be beneficial to provide a brief understanding of three critical aspects of the cybersecurity landscape that most oil & natural gas companies operate in.

First, the computer systems that make up the Industrial Control Systems (ICS) and operate our most critical components represent a significant risk concern. Today's ICS environments in the oil and natural gas industry rely on computing technologies for advanced control of unit processes (ex. Adjusting valves to regulate pressure or controlling pumps to regulate product flow) in refineries, petrochemical plants and pipeline/terminal distribution sites, which in turn makes them vulnerable to cyber-threats. For this reason, it is a widely accepted practice to ensure safety systems remain fully isolated from systems providing control of the unit. This basic tenet mitigates the risk of a cyber-threat to the safety of employees and the public in the physical surroundings of the plant.

Second, as with most businesses, we also rely on our internet-facing components, such as e-commerce for product purchases along with areas that allow collaboration with business partners. These components are contained in a part of our network that is outwardly facing to the public. We mitigate the risk of a cyber-threat to our internal network's exposure to the public internet by creating a security zone between the internal and external network that is frequently referred to as the DMZ. It uses this military reference because it exposes a portion of our network to the untrusted internet. A significant amount of security work is done to ensure only approved traffic flows between the DMZ and our internal network.

Third, our final focus area is on our internal network. This is the environment where our users perform functions such as email, collaboration, and analytics. It is here that we hold most of our intellectual property assets and conduct other internal business transactions. For the oil and natural gas industry, our most valuable intellectual property includes information regarding proprietary technology, break-through research, bid proposals, and acquisitions and mergers. Our cybersecurity focus in this area relies on early detection and a layered approach to defenses. User awareness training is also a critical focus area since we recognize that no amount of technology will protect us against every threat – the end-user provides a huge role as a layer in our defenses.

As a result of the many environments we operate in, threat-actors we face range from those commonly associated with financial gain (personal information and credit card theft), to those looking to protest ideological difference, to more dangerous adversaries associated with nation states interested in intellectual property theft or, in more extreme instances, physical destruction. The intellectual property of oil and natural gas companies can be frequent targets of nation state cyber-attacks because we operate critical infrastructure and often both compete and partner with the state-owned oil and natural gas companies globally.

Given the scope and impact cyber-breaches could have on operations, our industry has made protection from cyber-threats a significant priority. Specifically, API member companies share the concerns of policy makers regarding cybersecurity of the oil & natural gas industry – to protect critical infrastructure, to provide reliable energy for society and to safeguard public safety and the environment.

I can personally speak to the efforts within ExxonMobil and would like to highlight a few aspects that I believe have been instrumental in our work to provide a safe and secure computing environment.

1. Support for cyber-initiatives must come from the highest levels of management. We have been fortunate to have senior management that understands the importance of cybersecurity. This

support comes not only via funding, but also in security policy decisions and providing clear communications throughout the company that cybersecurity is a key focus area. A recent example of this can be found in communications from the business line presidents to their respective organizations regarding stewardship of careless actions where individuals fail to recognize malicious emails. Each business line is responsible for demonstrating actions to reduce the failure rate.

2. As noted previously, a layered defense approach provides the best protection in this rapidly evolving threat landscape. I am a firm believer that no one layer of defense or technology will ever provide 100% confidence regarding protection. Any attacker with enough resources and determination will likely discover ways to breach a single layer of defense. For this reason, we have employed a multi-layered approach, making the landscape much more challenging for an attacker to fully penetrate -- providing the necessary time to allow detective measures to respond.
3. Maintaining basic security hygiene is essential. ExxonMobil has a long history of risk management and controls compliancy, which we apply to cybersecurity as we have to other enterprise risks. These basic hygiene items include ensuring antivirus applications are up-to-date, security patches are applied and the use of powerful system IDs are managed for appropriate usage. This has paved a solid path for further enhancing our capabilities with respect to cyber-attacks, allowing us to focus on more sophisticated and challenging cyber-threats.
4. We have made some difficult choices in some instances to improve security over user productivity. Several years ago we made a case for restricting the use of removable media devices (ex. USBs, CDs) by providing data regarding the number of virus infections that were introduced into our environment via these devices. More recently, we have also used similar data to support restricting access to personal webmail from company workstations. While these initiatives were initially met with some apprehension, the resulting reduction in workstation infections and the increasing public awareness regarding significant cyber-attacks on other companies quickly allowed our user base to appreciate that these were effective and necessary actions.
5. Conducting periodic drills with key personnel has provided assurances that incidents can be detected, contained and remediated to avoid a significant loss. These drills include simulating a cyber-incident, such as a data breach, where an attacker has managed to gain some level of control over an internal computer, and is using it to steal sensitive files. These drills are typically unannounced and support personnel must utilize training to demonstrate the steps they would take to manage the event – which could entail reporting responsibilities both internal and external to ExxonMobil, depending on the type of data involved and the local laws that govern the situation. Additionally, developing plans to address a worst-case scenario ensures that we will be able to recover key computing infrastructure following a cyber-attack.

My recommendations to the committee are ….

1. Provide the infrastructure and processes to facilitate voluntary collaboration and information sharing of cyber-threats. ExxonMobil's work and relationship with the Department of Homeland Security (DHS) via the Cyber Information Sharing and Collaboration Program (CISCP) has demonstrated to us that the US Government is in the unique position to provide this service to the public and private sector in a way that is safe and secure.
    a. Information sharing of cyber-threat indicators is a critical defense because it strengthens an individual company's ability to know and counter current and potential attacks.
    b. For information sharing between and among companies and governments, supporting laws such as the US Cybersecurity Act of 2015 that provide the following legal protections to the

private sector: anti-trust exemption, limitations to public disclosure, limitations to liability and limitations to regulatory authority help foster sharing initiatives.

c. In order to be of maximum benefit, government sharing of information with the private sector should:

   i. Include reach-back to the intelligence community – coupled with requirements for companies to safeguard the privacy of personal information and to interface directly with civilian agencies.

   ii. Be unclassified as much as possible, i.e., without attribution of sources or methods.

   iii. Contain high fidelity and actionable indicators of compromise along with additional data such as attack type, date first seen in the oil and natural gas industry, extent seen in other industries, infection/detection rate, etc.

   iv. Also include some classified information, shared with individuals from the private sector with security clearances, in order to provide additional context for companies to anticipate and address future risks.

   v. Be shared with companies through a limited number of points of contact with government agencies while minimizing the duplication of information shared.

   vi. Ideally be conducted in real-time, machine-to-machine.

d. Considerations should also be made to support international information sharing given the global profile of companies' networks and commercial assets.

2. Continue to promote and enhance the Cybersecurity Framework, developed by NIST (National Institute of Standards and Technology) as the pre-eminent standard for companies' cybersecurity programs and for policy making globally.

   a. The NIST framework is comprehensive because its five core functions encompass the multiple dimensions required for an effective cybersecurity program – 1) Identify, 2) Protect, 3) Detect, 4) Respond and 5) Recover.

   b. The NIST framework's risk-based approach is consistent with the approach used to manage enterprise risk (i.e., those risks with the highest potential to cause harm to the company are given the most attention and highest level of control).

3. Encourage improvements in all technologies to ensure security is thoughtfully built into vendor provided products from the beginning and managed throughout the entire product life-cycle.

   a. Products should be fully tested for vulnerabilities by independent experts. It should be completely unacceptable for a product to enter the industrial environment that contains known vulnerabilities. Such cases result in unnecessary resources expended in efforts to mitigate these vulnerabilities after-the-fact.

   b. Vulnerabilities should be required to be quickly patched when public safety is at stake. When new vulnerabilities are discovered, patch development and delivery should be given a high priority and rapidly deployed. Products should also include processes to perform regular patches to address newly discovered vulnerabilities.

4. Take a measured and coordinated approach to any potential new cybersecurity laws or regulations, ideally based on a common understanding with industry on risks based on the Cybersecurity Framework.

   a. Laws or regulations should avoid a one size fits all approach. As noted regarding the Cybersecurity Framework, it allows companies to size solutions using a risk-based approach.

b. Additionally, setting a minimum standard via law or regulations can have a stifling effect on true advancements in technologies. If technologies only strive to meet the minimum standard, true innovation may not occur.

Thank you for allowing me to participate in this panel discussion. I look forward to addressing any comments and questions you may have.

Mark Webster

With the increasing reliance on information systems and the ever changing landscape of critical infrastructure's dependency on new and emerging technologies, industry and government agencies must ensure they are implementing best practices to protect their networks. Because critical infrastructure is a key component of our nation's security, the federal government has an interest in ensuring its protection. Adversaries are becoming more sophisticated in their cyber network exploitation and cyber network attacks. Therefore, the USG, its international partners, State, Local, Tribal and Territorial (SLTT) and industry, as whole, should recognize and implement the following techniques to efficiently and effectively protect their networks.

- Ensure software and firmware are patched promptly, and that critical infrastructure entities verify the integrity of and test those patches before applying them.
- Minimize the use of privileged user accounts and access. Only users who must have administrative (admin) privileges should have it, and those accounts should only be used when necessary. Admin accounts should be audited regularly.
- Establish a baseline of applications and security measures across all networks/hardware throughout the enterprise. The baseline can be a starting point for distinguishing between malicious and benign activity.
- In developing and structuring systems, care should be taken to segregate critical infrastructure systems from non-critical systems. Knowing what and where valuable information is stored or where critical infrastructure systems are managed is imperative for prioritizing network security.
- A final critical aspect of cybersecurity is formulating an incident response plan. This plan should take into account each step necessary to respond, when each step should occur, and who needs to be involved to ensure every step is carried out.
- Security measures go far beyond using tools/resources and implementing policies and procedures. A key part of cybersecurity often overlooked by industry is collaboration with the federal government, in particular the FBI. Establishing a trusted partnership with the FBI *prior* to a cyber event should be an integral part of any network security plan utilized by those who secure critical infrastructure systems. Why?
- Collaborating with the FBI and informing of intrusions or potential intrusions provides an opportunity for the federal government to surge its capabilities in addressing the malicious activity.