Carnegie Mellon University

Pacific Northwest NATIONAL LABORATORY

verizon

Compete. Council on Competitiveness

Cybersecurity

An Issue of National Security

Setting the Stage

On April 25, 2018, more than 50 experts across multiple sectors gathered to assess and make recommendations on the state of cybersecurity as it relates to U.S. national security. The second dialogue in a series of three explored the challenges and opportunities around protecting critical infrastructure from increasing cyber threats and identified some initial recommendations and areas for further analysis. This report, coupled with the first report, *Cybersecurity for Industry: Ensuring Prosperity in a Digital Economy* from the February 2 dialogue, will inform both the final dialogue on June 19 and a final report that will put forth a national strategy for cybersecurity to be shared with policymakers in Washington, D.C. and across the country.

CO-CHAIRS

Dr. Steven Ashby
Director
Pacific Northwest National Laboratory

Mr. George Fischer
Senior Vice President and Group President
Verizon Enterprise Solutions

Dr. Farnam Jahanian
President
Carnegie Mellon University

The Honorable Deborah L. Wince-Smith
President & CEO
Council on Competitiveness

Overview

The digitization of society, proliferation of data and increased connectedness of products and services—particularly in America's critical infrastructure sectors—have transformed the ways Americans live and organizations operate. Yet, the tremendous growth in the level of connectivity poses risks to U.S. global competitiveness as firewalls become the next frontline for battle in the United States. As a result, cybersecurity has become an issue of national security.

The United States is facing a steady increase in the volume, types and sophistication of cyber-attacks. Organizations of all types—including industry, government, academia and national laboratories—are assailed relentlessly by efforts from state and private entities to disrupt operations, steal information and increase their own competitiveness. These threats, which come in the form of traditional cyber-crime, military and political espionage, economic espionage and cyber warfare, carry considerable costs for the United States and the world. In fact, a study by Juniper Research suggests the annual cost of data breaches will reach $2.1 trillion globally by 2019, an increase of almost four times the estimated cost of breaches in 2015.[1]

Cyber-attacks are particularly concerning when it comes to the 16 critical infrastructure sectors as defined by the Department of Homeland Security[2]—each of which plays an integral role in America's economic and national security. A reliable energy grid, for example, is essential for any institution to operate. And while the U.S. Department of Energy currently has plans to improve preparedness, response and recovery capabilities, 90 percent of the energy grid is operated by private companies—requiring strong public and private partnerships to ensure these suppliers are resilient against and have the tools needed to respond quickly to potential cyber-attacks.[3]

The increasing sophistication of cyber-attacks poses a constant threat to critical infrastructure. And as the availability of networks is called into question every day, the economic viability of U.S. businesses and the freedoms Americans exercise daily are in jeopardy.

1 *The Future of Cybercrime & Security*, Juniper Research, March 25, 2017.

2 PPD-21 identifies 16 critical infrastructure sectors: chemicals; commercial facilities; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors; materials and waste; sector-specific agencies; transportation systems; and water and wastewater systems. https://www.dhs.gov/critical-infrastructure-sectors.

3 https://www.energy.gov/oe/activities/cybersecurity-critical-energy-infrastructure.

Initial Findings

Cybersecurity should be built into industry and government contracts to incentivize broader adoption. Cybersecurity must be better incentivized using new, innovative market mechanisms. This could include building security into procurement mechanisms or advancing how technologies are measured for security in order to institutionalize the adoption of security measures across the supply chain.

A unified, clear research agenda across industry and government is needed in the cybersecurity space. When it comes to cybersecurity research, there is no clear, community-defined research agenda, resulting in duplication of efforts and inefficient use of limited financial resources. A mechanism is needed to organize the research community and marshal appropriate stakeholders and topics to shape the research agenda.

Effort is needed to connect industry with laboratory and academic research to ensure knowledge transfer and reduce duplication. Discoverability of existing capabilities—both on the part of industry and the R&D community—is a significant challenge. Better coordination would reduce duplication of efforts—both within and across these communities—and help better align research priorities and commercial needs to scale up security solutions.

There must be a clearly-articulated federal model for cyber response to critical infrastructure attacks. While numerous government agencies are factoring cybersecurity into their programming and funding, there is minimal coordination across these programs. This would decrease duplication of efforts and improve resiliency and response capabilities in the face of cyber threats.

There is an opportunity at the state or regional level to capitalize on the patriotism, altruism and tech-savviness of younger generations to create coalition(s) of cyber first-responders. Current recovery times from cyber-attacks are long and static, threatening American security and economic interests. The United States needs a coordinated first-response effort to further regional cyber protection and response. One potential home for this effort could be within the National Guard.

Globally-defined, security baselines are needed and must be informed by relevant stakeholders. Useful and practical security baselines would level the playing field and set basic expectations around how systems and networks can be deployed in recommended, secure configurations. Advances must be made through the product lifecycle to improve design, default and deployment, thereby building assurance around the resiliency of critical infrastructure to cyber-attacks and disruption.

Applying automated security monitoring to critical infrastructure sectors would significantly improve cyber defense. When applied to the observe-orient-decide-act loop, continual evaluation of security through artificial intelligence and machine learning can enable adversary detection, attribution and action prediction and improve response in a way that would reduce the asymmetric advantage of attackers and level the cyber defense playing field for critical infrastructure providers.

Cybersecurity must be integrated into the academic curricula of related topics. While training cybersecurity professionals is a valuable endeavor, cybersecurity must be a key educational component for computer scientists, engineers and other professions in which security is a foundational concern. This will increase the pool of professionals with relevant and applicable cybersecurity skills across the most critical areas of need and ensure that future engineers across all disciplines are able to design and build secure systems.

Barriers prohibiting practitioners to serve as educators must be reduced. While there are significant challenges around a mismatch between supply and demand of cybersecurity professionals, academia faces the compounding challenge of a lack of educators to train the workforce of tomorrow. A strategic effort on the part of industry and academia is needed to fill this gap.

Key Themes

Securing America's Critical Infrastructure

Cybersecurity should be built into industry and government contracts to incentivize broader adoption.

The need for security-conscious, comprehensive solutions to the challenges presented by increasing interconnectedness and the proliferation of data is not a new phenomenon. Looking back as far as 1997, scholars and practitioners warned of relying on "silver bullet" solutions to security challenges. While there has been progress increasing resiliency to cyber threats, the number of unaddressed recommendations in any number of studies continues to grow.

The 16 critical infrastructure sectors are grouped together and defined as those with physical and virtual assets, systems and networks considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national and/or economic security, national public health and/or safety. This construct, while helpful for looking at macro-level security challenges, can sometimes hide the intricacies of these challenges. Understanding how each sector connects to the critical functions it supports—and how the sectors connect to and support one another—is essential for creating a resilient ecosystem.

While cyber-physical events are commonly thought of as the biggest security risk to critical infrastructure, increasing reliance of business functions on IT networks has created a new frontier of vulnerabilities; one where disruptions can be even more detrimental. By disrupting functions that, in themselves, might not have a physical consequence but that impact the ability to provide basic needs, adversaries can severely harm American economic activity and daily life.

Security weaknesses are prolific when it comes to design implementation. As a nation in which, unlike many others, the private sector owns 87 percent of energy and produces many of the devices used by military, it is essential to create baseline security standards and incentivize private sector cooperation and information sharing. Yet, disclosing security vulnerabilities opens companies up to liabilities and reputational risk. Additionally, as companies grow and begin to build increasingly complex products by expanding their use of varying software programs, it becomes increasingly more important to manage to simplicity rather than complexity. If the market continues to focus on creating space for future products, driving companies to seek complex solutions when simple ones are available, interoperability between systems and programs becomes extremely challenging. This creates an important role for government to create standards protecting the security of critical devices and operations along the supply chain.

Policymakers have taken steps to protect America's critical infrastructure, including as far back as the Recovery Act of 2009, which supplied grant money for smart grid investment. Within this grant, 100 smaller grants were issued by the U.S. Department of Energy that carried the requirement of a cybersecurity plan from recipients. More recently, the Securing Energy Infrastructure Act, introduced in 2016 and sponsored by Senator King, sought to address the issues facing the current system, such as general purpose computers running the electric grid. However, this legislation neglects to address the technology in place to disrupt potential attackers or encourage the use of appropriate add-on security technology.

The way vendors and consumers view security also impacts America's overall security posture. New, innovative market mechanisms—including procurement mechanisms, standards and other activities that advance the way in which technologies are measured for security—could incentivize vendors to view cybersecurity as a competitive advantage. But at the same time, vendors tend to favor consumer demand and preference. Until consumers consistently demand security, government procurement measures alone cannot solve the problem.

So, while there are numerous challenges around securing America's critical infrastructure from cyber-attack threats, increased recognition on the part of policymakers, industry and academia is encouraging. It is clear the question is no longer "if," but "how" America can secure its critical infrastructure from increasing cyber threats.

The Innovation Cycle: From Idea to Implementation

A unified, clear research agenda across industry and government is needed in the cybersecurity space.

Effort is needed to connect industry with laboratory and academic research to ensure knowledge transfer and reduce duplication.

It is often argued that the United States does not have an innovation problem but an adoption problem. An undefined cybersecurity research agenda, varying investment priorities and difficulties around discoverability and duplication of existing intellectual property are just some of the challenges researchers and companies face when developing and implementing new cybersecurity capabilities. While each is a distinct challenge, improving coordination between industry, academia and government and addressing the innovation system holistically would vastly improve U.S. security posture and competitiveness.

One of the most confounding cybersecurity challenges facing the research community is the lack of a unified, community-defined research agenda. One way to create consensus-driven prioritization of research questions—and illuminate long-term challenges that are unlikely to be solved by the private sector—is by leading a Basic Research Needs workshop, similar to those conducted by the Office of Science at the U.S. Department of Energy. These workshops bring together experts to define Proposed Research Directions that address the technology R&D challenges and define the grand challenges that, if solved, might result in transformational changes in technologies. While these efforts are being undertaken in specific parts of cybersecurity, such as grid security, a broader effort to prioritize the allocation of limited federal dollars in the cybersecurity sphere is necessary.

When it comes to financing innovation, investment priorities between venture capitalists and government R&D funding differ vastly. While venture capitalists typically derive a majority of their profit from a select few investments, military and government R&D dollars demand innovation in an environment in which failure is not an option. Government investments are often made through technology foraging efforts such as Transition to Practice (TTP) programs. These programs seek to: identify promising technologies that address an existing or imminent cybersecurity need impacting national security; increase utilization through partnerships, product development efforts and commercialization; and improve the long-term ability of federal government research organizations to transition technology more efficiently.[4] While TTP programs signal a step in the right direction in terms of coordination, the current size of these programs is inadequate to solve the growing cyber threat challenges.

Additionally, when it comes to government-sponsored R&D, agencies often have varying appetites for supporting the transition of capabilities to the private sector. While some are eager to actively support the licensing and transition of cybersecurity tools to companies that can take them to market and help them see broader effect, others prefer to reserve new innovations for their exclusive use. The risks and benefits of making a new innovation widely available to the nation's critical infrastructure versus keeping new cybersecurity innovations restricted to a particular field of use or a particular national security mission must be more openly discussed among technology funders.

Discoverability of existing capabilities and intellectual property is another challenge in the cybersecurity sphere. This is true in both directions between the R&D community and end users, as well as internally within each of these communities. For researchers, understanding the needs of the end user community—and appropriate transition opportunities—proves to be a persistent challenge. For end users, discovering useful products and connecting with universities and national laboratories poses a significant challenge, as does understanding existing research largely produced and written by academics and scientists with minimal business acumen. Making the university research agenda both more

4 https://www.dhs.gov/science-and-technology/csd-ttp.

openly available and comprehensible to corporate decision makers would improve the ability of companies to plan for integration of on-the-horizon technologies into future products, avoid duplication and, at the same time, identify potential partners.

Ultimately, when it comes to innovation, there is no replacement for good requirements and good data. However, the question of what exactly should be measured in order to show quantifiable value of cybersecurity capabilities is still uncertain. Closely pairing researchers with operational customers is one way to get over the hurdle of unclear requirements or insufficient data. Alternatively, seeking out researchers with both practitioner skills and an innovative spirit makes it easier to close the loop from early stage research to developing and engineering products to prove research in test beds. These solutions can be deployed in an operational community. Ultimately, each of these challenges requires coordination and collaboration in order to improve America's resiliency and recovery in the face of cyber threats.

In Search of Best Practices

Maj. Gen. Tim Lowenberg National Guard Cyber Defenders Act

In September 2017, U.S. Representatives Derek Kilmer (D-WA) and Steven Palazzo (R-MS) introduced bipartisan legislation that would create Cyber Civil Support Teams (Cyber CST) through the National Guard to coordinate responses to significant cyber-attacks in their states. While there are currently units available when an incident requires a federal response, many states lack separate teams that can respond to cyber-attacks compromising their infrastructure.[1]

Washington State Military Department

The Washington State Military Department has worked aggressively to prepare the state for cyber emergencies. Extensive outreach and program development efforts by the National Guard and other state agencies culminated in the creation of a Cybersecurity Program within the Emergency Management Division. The manager of the program functions as the state's cybersecurity policy leader and strategist for emergency management. This is perhaps the first real blending of cyber and emergency management in the United States to fully integrate cybersecurity into statewide emergency planning, training, preparation, and response procedures and could serve as a model for state-level emergency response efforts.[2]

Area Maritime Security Committee

In 2002, in response to the September 11, 2001, terrorist attack, the Department of Homeland Security established the Maritime Transportation Security Act to protect maritime critical infrastructure from the threat of attack. Under this act, AMSCs were established to enhance communication between port stakeholders within federal, state and local agencies, and industry to address maritime security issues. This model could be used to establish cybersecurity committees to encourage strategic cooperation and rapid response to threats.[3]

1 https://kilmer.house.gov/news/press-releases/representatives-kilmer-and-palazzo-introduce-bipartisan-legislation-to-create-national-guard-cyber-units-to-help-states-counter-cyber-attacks.

2 https://mil.wa.gov/emergency-management-division/cyber-security-program.

3 https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/amsc/.

Coordination and Collaboration in an Age of Cyber Threats

There must be a clearly-articulated federal model for cyber response to critical infrastructure attacks.

There is an opportunity at the state or regional level to capitalize on the patriotism, altruism and tech-savviness of younger generations to create coalition(s) of cyber first-responders.

When it comes to collaboration and threat coordination in the cybersecurity space, challenges may often seem intractable and unmanageable to single agencies, companies and universities—many of which are attempting to tackle similar problems at the same level. Resolving these challenges requires better use of limited research dollars through more coordination across industry, academia, the national laboratories and the various government agencies.

There are examples of strong partnerships at the state, regional and sector levels, but scaling and replicating these initiatives is challenging, with a lack of trust hindering coordination more so than technical challenges. But with the corporate firewall being the next battle frontline for the United States, coordination and collaboration are needed to mitigate the cascading consequences of potential cyber-attacks. Additionally, the R&D community often lacks the skills needed to communicate effectively with operational customers—to ask the right questions, understand emerging needs and communicate the value of new technology in the context of mission requirements—creating knowledge gaps across the two sectors.

As global competitors continually build up their resilience to cyber threats and, in some cases, their adversarial capabilities, the United States is in need of a top-down, grand strategy for cybersecurity. As a first line of defense, however, policymakers must realize and capitalize on the value of practicing cyber deterrence as a protection strategy. Cybersecurity has been kept behind the wall as an IT problem for far too long; openly discussing cyber-readiness can create a perceived resiliency among potential adversaries.

When it comes to building resiliency to cyber-attacks across the 16 critical infrastructure sectors, the ends, ways and means must be pulled together in a way that considers diplomatic, informational, military and economic priorities. The National Guard presents an opportunity to integrate military and industry best practices and apply them in the cybersecurity space, perhaps serving the role of cyber first responder. Globally, organizations such as Estonia's cyber militia could serve as a model, as could the public-private cyber resilience coalition, Cyber Incident Response Coalition & Analysis Sharing (CIRCAS). While there are currently a number of institutions with Guard members on staff, this is typically driven by individual preference. Institutionalizing partnerships between the Guard and the private sector would create opportunities for active recruiting and sourcing at the institutional level to ensure a reliable source of talent over time, while leveraging millennial patriotism.

While industry, particularly large corporations, is largely responsible for responding to cyber threats, the government is often tasked with filling a coordination role, as well as fill in gaps by bolstering the capabilities of small-holder owners of critical infrastructure through grants and other types of support. The challenge therein lies in defining a clearly-articulated federated model for responding to cyber-attacks on critical infrastructure. This has been unsuccessfully attempted in the past, with various agencies claiming the lead in different instances. Better inter-agency coordination and a clear leading voice on cybersecurity issues within the government are needed in order to improve the overall threat deterrence and response capabilities of the United States.

Cybersecurity: From Cost to Competitive Advantage

Globally-defined, security baselines are needed and must be informed by relevant stakeholders.

Applying automated security monitoring to critical infrastructure sectors would significantly improve cyber defense.

Attackers of all shapes and sizes—from individuals to nation-states—are constantly seeking to exploit security gaps through traditional cyber-crime, economic espionage and cyber-warfare. These adversaries have various motivations, including financial gain and IP theft. Hackers are often able to enter a system and exfiltrate data within minutes. Of greater concern, however, is that it can take months for a company, national laboratory, the government or any other entity to detect and contain the threat. According to the most recent Ponemon Cost of a Data Breach Study, in 2017 it took U.S. companies an average of 206 days to detect a data breach and an average of 55 days to contain them. And with the average cost of a data breach in the United States at an all-time high of $7.35 million, these attacks are detrimental to productivity.[5]

Two of the factors contributing to extended response and remission following a cyber-attack are a lack of baseline security standards and a tendency to view security as an issue of compliance rather than risk management. Government-developed security baselines can be both positive and negative. When designed to address pre-defined security outcomes through a collaborative process that includes diverse stakeholders, security baselines can level the playing field and set basic expectations around how systems and networks can be deployed in recommended, secure configurations. Yet, baseline requirements can also lead to a compliance-based culture rather than outcome-based solutions to security challenges. This must change from the start of the procurement process.

While there are challenges facing companies and organizations of all sizes, small companies and new tech startups tend to find themselves with larger hurdles to overcome. Designing with security in mind, and the associated costs of building security into products, is oftentimes a constraint for small, yet innovative, companies that lack the resources available to larger entities. With many of these companies striving to push minimally viable products, which contain little to no security measures, into the marketplace, there is a need for these innovative companies to begin considering security as a necessary component. Public-private partnerships to encourage information sharing across companies of different sizes is crucial for smaller companies, as it allows them to learn from and leverage the existing knowledge and resources of large enterprises.

Sharing threat information across companies on a real-time basis is perhaps the best way to raise the overall security posture of American industry. The recently-announced "Tech Accord," an effort by a group of more than 30 companies to lay out basic principles for cooperation and to encourage industry partnerships, is one attempt to improve information sharing. One idea stemming from the Tech Accord is a digital Geneva Convention, which would set up new international norms and a framework for how governments can work together to counter instances of cyber-attacks. It does not, however, include the public sector voice despite its position as a key player in securing American interests from the threat of cyber-attacks. And while agreements such as the Tech Accord are certainly moving the conversation and relevant parties in the right direction, it remains to be seen whether these efforts can make the long-term impact necessary to improve resilience.

While baselines, standards and cross-sector collaboration are pieces of the puzzle, there must also be improved cooperation between IT and operational technology teams. Moreover, there must be increased efforts to move security to the left of the technology lifecycle during the design and architecture phases of IT projects, which is significantly less expensive than treating security as an add-on.

5 *2017 Cost of a Data Breach Study*, Ponemon Institute, July 2017.

While security measures are considered table stakes when it comes to IT, security can be sold as a differentiator given the existing metrics. When it comes to operational technology (OT), however, there are risks to implementing new security measures, including system downtime and incompatibility between older hardware and new security technologies.

Additionally, when it comes to monitoring security threats, utilizing automation and machine learning technologies is vital. Applying automated security monitoring to critical infrastructure sectors would significantly improve security posture. When applied to the observe-orient-decide-act loop, continual evaluation of security through artificial intelligence and machine learning can reduce the total number of cyber-attacks and reduce the time to remediation following a cyber-attack. Though sensors, videos and other technologies can be a cost-effective mechanism for reducing human error and providing continuous information, digitization comes with a risk when these technologies become more trusted than people. A balance must be struck to keep a human in the loop to maintain thoughtful perspectives over processes.

While notable efforts such as agreements and renewed focus from both private and public entities indicate forward progress, private organizations and governments need to maintain focus on building and implementing security and resilience measures and standards that protect crucial sectors from cyber threats.

Next-Gen Talent: A Cybersecurity Imperative

Cybersecurity must be integrated into the academic curricula of related topics.

Barriers prohibiting practitioners to serve as educators must be reduced.

It is vitally important that the United States has an adequate, viable cybersecurity workforce to secure critical infrastructure, but also to address a myriad of national security and domestic concerns. The race to respond to cyber workforce needs has led to inconsistency in program quality and stove piping of expertise. The ability of academia, industry and government to address these challenges collectively while meeting current and future needs will be a key driver of American competitiveness in this burgeoning field.

Cybersecurity is constantly evolving, creating higher demand for talent and shifting the skills required to deal with new actors and challenges. This creates challenges for existing members of, and new entrants into, the cybersecurity workforce, who are often unable to keep pace with these changes. At the same time, cybersecurity is still in its youth as an academic discipline, and the methodologies deployed by academia lack the consistency and discipline needed to cover the growing talent gap.

There is currently a vast divide between the available qualified workforce and the number of jobs that need to be filled. Currently, the United States is falling behind in educational spending, while countries like China and South Korea are increasing investments in training cybersecurity workers. While cooperative learning and apprenticeships can increase the talent pool, the demand for cybersecurity professionals already exceeds supply.

The lack of available talent has led to worker poaching—workers leaving jobs in search of higher pay and more prestigious positions. A cooperative learning model, augmented by personal mentoring, allows for students to gain the needed knowledge. Meanwhile, this model fosters a connection to the company that encourages loyalty to the organization after graduation, creating a measurable return on the time investment on the part of the company. If scaled up, this model could help mitigate fierce competition for limited talent and ensure workers are graduating with the skills needed.

But increasing the supply of young professionals entering the cybersecurity field is not, on its own, enough to fill the growing talent gap. There is a need for continuing education opportunities to reskill workers and capitalize on under-utilized pockets of excellence. One such example is service women and men transitioning out of the military who might want to enter cybersecurity-related

second careers. Additionally, online curricula, professional education models and community colleges must all be considered as viable paths to encourage lifelong learning opportunities.

Along with the deficit in talent in the workplace, there is an equally important deficit in instructors. One way to increase the number of practitioners is to draw from other fields, such as bioscience and mathematics, where the presence of analogous problems would lessen the burden of training these professionals to teach cybersecurity topics. Encouraging students to enter academia after college, or creating an option for professionals seeking to transition out of the industry workforce, would also help increase the pool of cybersecurity instructors. Combined with cooperative and continuous learning opportunities, this would address some of the root causes of the growing gap between supply and demand of cybersecurity talent.

There must also be a concerted effort to integrate cybersecurity into computer science, engineering and other technology-based academic fields. By creating a cadre of cybersecurity specialists, there is a risk of misalignment with a market need for young professionals who can apply cybersecurity principles to their respective functions. Bringing cybersecurity into other fields is necessary to create a well-rounded workforce that is able to utilize cybersecurity in a practical manner upon entering the workforce and to ensure future engineers across all disciplines are able to design and build secure systems. Competitions that encourage cross-disciplinary teams to address grand challenges are another method of cross-pollinating skills. This integration would also bring fresh ideas into the innovation cycle, pushing cybersecurity forward to new levels of success.

Compete.
Council on Competitiveness

Council on Competitiveness
900 17th Street, NW, Suite 700, Washington, D.C. 20006
T 202 682 4292
Compete.org

@CompeteNow
facebook.com/USCouncilonCompetitiveness
linkedin.com/company/council-on-competitiveness/

Cybersecurity Dialogue 2 Participants

Dr. Heidi Ammerlahn
Director, Homeland Security & Defense Systems
Sandia National Laboratories

Dr. Steven Ashby
Director
Pacific Northwest National Laboratory

Mr. Jeffery Baumgartner
Senior Advisor, Infrastructure Security and Energy Restoration
Department of Energy

Ms. Marie Benz
Client Partner
Verizon

Mr. Randy Bishop
General Manager—Energy Infrastructure
Guardtime

Mr. Craig Bowman
Vice President and Managing Director
Verizon

Dr. Lloyd Wayne Brasure
Director, Defense Programs
Pacific Northwest National Laboratory

Ms. Margaret Brooks
Senior Manager, Risk Management
Verizon

Mr. James Carrigan
Managing Director—Security Solutions
Verizon

Mr. Samuel Clements
Cyber Security Researcher
Pacific Northwest National Laboratory

Mr. Jerry Cochran
Chief Information Security Officer
Pacific Northwest National Laboratory

Mr. Paul Cunningham
Chief Information Security Officer
Department of Energy

Dr. Jim Davis
Vice Provost, Information Security
University of California, Los Angeles

Mr. Paul Dodd
Senior Technical Fellow
The Boeing Company

Mr. Seth Edgar
Chief Information Security Officer
Michigan State University

Dr. Barbara Endicott-Popovsky
Executive Director
Center for Information Assurance and Cybersecurity

Mr. Mark Estberg
Senior Director
Microsoft

Mr. Daniel Freedman
Fellow—Cyber Security
Lockheed Martin

Mr. Michael Furze
Assistant Director
Washington State Department of Commerce

Mr. Scott Godwin
Strategic Partnerships and Delegate Initiatives
Pacific Northwest National Laboratory

Mr. Victor Gonzalez
Chief Information Security Officer
South Texas College

Mr. Robert Hanson
Director, Prioritization and Modeling
Office of Cyber and Infrastructure Analysis, Department of Homeland Security

Mr. Carl Imhoff
Manager, Electricity Infrastructure Sector
Pacific Northwest National Laboratory

Dr. Susan Jeffords
Vice Chancellor of Academic Affairs
University of Washington-Bothell

Ms. Kristen Lantz
CTO Operations Lead
Lockheed

Ms. Aimee Larsen-Kirkpatrick
Global Communications Officer
Global Cyber Alliance

Mr. Steve LeFrancois
Director, Solutions Architecture
Verizon

Dr. Sukarno Mertoguno
Program Officer
Office of Naval Research

Mr. Matthew Myrick
Deputy Chief Information Security Officer
Lawrence Livermore National Laboratory

Mr. Alex Nicoll
Industrial Security Architect
Rockwell Automation

Dr. James Peery
Global Security Directorate Associate Laboratory Director (ALD)
Oak Ridge National Laboratory

Dr. William Pike
Director, Computing and Analytics Division
Pacific Northwest National Laboratory

Mr. Daniel Roat
Senior Client Executive
Verizon

Ms. Heather Scott
Office of Cyber and Infrastructure Analysis
U.S. Department of Homeland Security

Ms. Bobbie Stempfley
Director, SEI CERT Division
Carnegie Mellon University

Mr. Clay Storey
Senior Security Manager
Avista Corporation

Rep. Gael Tarleton
Representative
Washington State Legislature

Mr. Zachary Tudor
Associate Laboratory Director, National & Homeland Security
Idaho National Laboratory

Mr. David Walter
Chief Operating Officer
Leisnoi, Inc.

Col. Gent Welsh
Commander, 194th Wing
Washington National Guard

Dr. William Wescott
CEO
Brainoxygen LLC

Ms. Jamie Winterton
Director of Strategy, Global Security Initiative
Arizona State University

Ms. Morgan Zantua
Director, Professional Workforce Development
Center for Information Assurance and Cybersecurity

Mr. Chad Evans
Executive Vice President
Council on Competitiveness

Ms. Katie Sarro
Senior Policy Director
Council on Competitiveness