NEW DEMS

Safeguarding Our Economy and Our Future

Cybersecurity Task Force, New Democrat Coalition

Co-Chairs: Representatives Derek Kilmer, Kathleen Rice, Josh Gottheimer

Our economy and society are increasingly dependent on technologies such as the Internet, smartphones, and cloud computing, and as technology evolves, so do cyber threats. Recent high-profile cyber incidents—such as the Russian interference in the 2016 election, the breach at Equifax that compromised the personally identifiable information (PII) of 145.5 million people, the breach of the Securities and Exchange Commission, email database breaches, and the rise of ransomware—have shown the very real consequences of cyberattacks. The future of our nation's economy, security, and our very democracy will depend on our ability to effectively operate in the cyber domain.

Confronting digital security challenges has been and remains critical for our national security. Just as the National Institutes of Health and the Centers for Disease Control work to advance research and responses to public health epidemics, the federal government needs a mechanism to better safeguard the public against cyber threats and better monitor threats against the federal government. It is time for the country to develop a comprehensive cyber strategy.

Threats from cyberattacks are diverse and affect many parts of our society, making it difficult for any single congressional committee to craft a comprehensive response. The New Democrat Coalition created the Cybersecurity Task Force to cut across siloed committees and develop a robust cyber policy plan. In producing this paper, the Task Force collaborated with industry experts, thought leaders, and government agencies to identify several key issue areas and policy proposals.

In this report, the Task Force focuses on how to leverage public-private partnerships, such as those established under the Cybersecurity Information Sharing Act (CISA) that focus on resiliency and risk management, to strengthen our nation's cyber defense and foster the development of greater cybersecurity both within the government and outside of the regulatory bureaucracy. The report is organized around five central themes:

1. ***Fostering and encouraging public-private and industry-wide information sharing;***
2. ***Developing stronger defenses and partnerships to protect critical infrastructure against cyberattacks;***
3. ***Developing a strong cyber workforce pipeline and attracting them to both the private and public sectors;***

4. ***Investing in and developing stronger technologies and defenses for data and information security at the public sector, private sector, and individual levels;***
5. ***Securing and defending the Internet of Things (IoT).***

Vulnerabilities and attacks will always exist, so aptly responding to and planning for the future are key. That means identifying the right way to detect, isolate, resolve and ultimately minimize the effect of an attack. Additionally, legislation cannot solve all problems. Heavy-handed regulation can hinder innovation and new start-ups from entering the market. Congress, the executive branch, and industry must constructively work together to foster a more secure and effective cyber environment that allows continued commercial, civil, and social interactions and innovations on which American society depends.

Information Sharing

The sharing of cyber threat information is a vital component of both cyber resiliency and risk management. Information sharing allows different companies, sectors, and government entities to better prepare for and respond to threats and to better understand "how" incidents happen more than "why." Prompt information sharing also has the power to disrupt the economic incentives of cyber threat actors by enabling other individuals, companies, and organizations to identify how an incident has occurred and defend against an attack. While the private sector must cooperate for information sharing to be truly effective, the government must do more to become an effective partner for the private sector. Communication cannot simply be a one-way street, in which one side shares its data but receives little to no new information in return. Similarly, information sharing needs to occur in a timely, actionable way for it to be truly effective. To facilitate this information sharing partnership, we propose the following policies and actions:

- ***Identify the information resources available to the private sector from the government, and demonstrate the value of information sharing.***
- ***Enlist the organizations that span state and federal governments in fostering relationships between the private and public sectors.***
- ***Improve the legal framework concerning the security classifications of cybersecurity information to more quickly declassify and release critical information to the private sector as appropriate.***

Trust is a necessary component of information sharing. Cybersecurity experts and professionals responsible for critical systems are understandably hesitant to allow unfamiliar people access to their networks. However, given how intertwined the public and private sectors are, we need to encourage communication and trust. By enlisting organizations that span the local, state and federal governments—such as the National Guard—to facilitate communication and cooperation between the private and public sector, the government can expand upon the existing goodwill and relationships of organizations and agencies that work locally but are part of a national network. The Cybersecurity Information Sharing Act authorizes and provides a limited safe harbor for private entities to voluntarily share threat information and defensive measures with each other and the federal government. The Task Force will work to ensure that CISA incentivizes meaningful information sharing that prevents or limits the impact of attacks. While the program is relatively young, it has been underutilized. More work must be done to encourage and enable the private sector to partake in information sharing, and to foster dialogue with the federal government. We cannot allow our cybersecurity framework to jeopardize the very freedoms we are fighting to protect, and we are encouraged by the steps CISA takes to enable information sharing without sacrificing privacy protections.

The government needs to recognize the risk and cost for companies to participate in information sharing endeavors. Industry has reporting requirements from federal, state, and local governments, as well as from sector specific rules, which collectively take up significant time and resources. The government needs to better articulate the available resources and demonstrate the value of these partnerships.

The Federal government should work with the private sector to balance the important need to protect sensitive information and methods while balancing the need to share pertinent information to warn and protect industry and individuals from serious cyber threats. The Vulnerabilities Equities Process (VEP), which is overseen by the National Security Council, is an interagency process used to determine whether to disclose certain cybersecurity information and vulnerabilities, but it is not codified. Government agencies need to improve the legal framework outlining the sharing and, where appropriate, declassification of information. A challenge for entities that receive classified material is the ability to act on that information without divulging it to individuals lacking the appropriate clearance level. Obtaining security clearance is a difficult and lengthy process, and therefor declassifying critical information in a timely manner can help industry swiftly and effectively respond to a potential cyber threat. DHS should work with other national security apparatuses to increase appropriate sharing of information through VEP, and increase the prompt declassification of information as appropriate.

Critical Infrastructure

As more and more components of our infrastructure systems rely on interconnected technologies to function, the potential impact of cyberattacks has grown dramatically. The Department of Homeland Security (DHS) has identified sixteen sectors of critical infrastructure vital to the United States, and which, if incapacitated, would significantly impair the U.S. national security, economy, and/or public health and safety. A consensus has emerged that DHS, as a civilian agency, is the best positioned federal department to sustain this cooperation and lead the government on cybersecurity. Because the private sector and state or local governments own and operate most of our critical infrastructure, we need strong channels of communication and collaboration between the public and private sectors, and between different levels of government. The New Democrat Coalition Cybersecurity Task Force has identified a set of proposals we believe can strengthen and secure our critical infrastructure:

- ***Improve and develop streamlined public-private partnerships to:***
    - ***Share data and information;***
    - ***Test and model critical infrastructure vulnerabilities; and***
    - ***Develop resilient critical infrastructure systems.***
- ***Direct the National Guard to establish Cyber Civil Support Teams to respond to and advise on significant state and local cyber incidents under the direction of the state's governor, and provide funding for the recruitment and training of National Guard cyber threat responders.***
- ***Encourage state and local authorities to work with and accept the help of federal agencies, including DHS.***

- ***Encourage various entities involved in our electoral system to work with state authorities, DHS, and the intelligence community to develop an understanding of and response to attacks on our election systems and democracy.***

For years, leaders in every sector have sounded the alarm about the need for improved cybersecurity. While more must be done defensively to protect critical infrastructure sectors from cyber criminals and state-sponsored attacks, we also must focus on resilience. We need to have systems in place that can quickly and effectively respond and are built to adapt and rebound. DHS should encourage improvement of sector-specific efforts—and development of cross-sector efforts where appropriate—within the private industry to develop and maintain critical infrastructure systems that can be restored efficiently after an attack. This resiliency approach will allow us to ensure continuity of essential services and economic activity.

The federal government has laid a good foundation through programs such as the DHS Computer Emergency Readiness Teams to respond to cyber emergencies. These existing federal programs and teams, however, could benefit from better consistency and funding. To further support the existing efforts and cybersecurity response structures of the DHS, the Federal Emergency Management Agency (FEMA) could establish a dedicated grant program to assist state, local, and tribal governments in preparing for, protecting against, and responding to cyber threats. Furthermore, because of the nature and structure of these programs, states must also develop their own plans for preventing, preparing for, and responding to a cyber incident. The preparedness of states varies drastically across the country but we are only as strong as our weakest link.

In early 2017, election systems were designated as a subsector of the existing Government Facilities critical infrastructure sector. While state and local governments have central roles to play in strengthening cybersecurity preparedness and response structures, they must also recognize the limits of their capabilities in the event of a cyberattack from a nation-state actor. Our free and fair elections are a cornerstone of American democracy. Following Russia's attempted hack of the election systems of 21 states during the 2016 election, states should be willing to accept help from DHS to ensure secure elections in the future.

Public-private partnerships can aid in testing critical infrastructure vulnerabilities and further promote existing structures of federal- and state-level collaboration. This strategy was proven successful in Washington State when the Snohomish County Public Utilities Department and the Washington State National Guard worked with a private company to model and simulate a cyberattack. The final report from this partnership included an assessment outlining the probability of certain attacks, the projected cost of attacks, and a list of actionable risk-reduction ideas.

Because cybersecurity is a federal national security priority, we must recognize and address disparities in individual states' abilities to respond to cyberattacks. Existing capabilities, such as the Department of Defense's Cyber Protection Teams, are federally-tasked and, although they could respond to state level cyber incidents, they generally are activated for federal missions. As demonstrated in the partnership with Snohomish County Public Utilities Department, the National Guard is well-positioned to fill this gap. The National Guard should replicate the existing Civil Support Team structure and create Cyber Civil Support Teams to coordinate responses to significant cyber incidents in their state or region acting under the direction of their respective governors. The federal government should also provide funding to assist in the recruitment and training for these Cyber Civil Support Teams. The considerable goodwill and trust the

National Guard and its Civil Support Teams have established in their local communities make them excellent bridges between the federal government and states.

Cyber Workforce

The cybersecurity workforce is the front line for tackling these evolving problems, and our approach to building and maintaining an agile workforce needs further investment and development. Government job requirements are outdated and too rigid, and job categories need more consistency across agencies. In addition, government hiring authorities need more flexibility to recruit and retain qualified cyber professionals, especially when faced with formidable competition from the private sector. Yet even the private sector is struggling to find qualified candidates that meet the existing criteria. Through discussions with industry leaders and the review of several reports, the New Democrat Coalition Cybersecurity Task Force has identified a set of proposals we believe can better develop and engage the cyber workforce:

- ***Incentivize the government to actively attract and recruit underrepresented groups to the cybersecurity field.***
- ***Invest in STEM education and include basic cyber hygiene within our education system for grades K-12.***
- ***Encourage non-traditional education paths, such as two-year degrees, apprenticeships, certification training, and testing programs developed in partnership with industry.***
- ***Expand the ability of government agencies to pay for certification training.***
- ***Establish a new national service program that forgives federal student debt for STEM graduates who go to work for the federal government in cyber and information technology positions.***
- ***Identify cyber skillsets and training within the military to allow servicemembers and veterans to transition into cyber fields within the civilian workforce and government.***
- ***Partner with the private sector and educational programs to develop consistent cyber job taxonomies.***

One way to fill gaps in the workforce is to expand the talent pool and create opportunities for traditionally underrepresented groups such as women and minorities in the cyber and technology field. The 2017 Global Information Security Workforce Study report, *Women in Cybersecurity,* found that women constitute only 11 percent of the cyber workforce. Including STEM education and basic cyber hygiene skills in school curriculums from an early age would introduce the field of cybersecurity to a diverse population of students and expose them to an exciting future career path. By encouraging all students—regardless of gender, race, or background—to pursue STEM fields, the U.S. can address its cyber workforce recruitment and diversity issues and improve the overall cyber ecosystem.

Today there is a broader range of jobs within the cyber profession than traditional high-skill roles, creating opportunities for individuals with cybersecurity and technology skills acquired outside of traditional four-year degrees. While there is still a need for individuals with advanced or specialized training, there is substantial demand for tactical-level workers with less formal education, such as two-year degrees or certification training.

In the private sector, certification testing is a great mechanism for recruiting candidates who may not have a traditional four-year degree. These certifications are created by industry, in collaboration with executive branch agencies such as the National Institute of Standards and Technology (NIST), and prove valuable in a multitude of ways. Industry can readily adapt certification testing and training programs to these changes in workforce needs and, building off of the work of NIST's National Initiative for Cybersecurity Education (NICE) Framework, create uniform job taxonomies and requirements that are directly correlated to the syllabi of training programs.

These certifications can also be used as a tool to recruit and retain cyber professionals in the federal government. Expanding the ability of government agencies to pay for certification training—and expanding the eligibility of programs—would incentivize qualified, skilled individuals to work for the government. These certifications provide clear pathways and opportunities for professional development and career advancement.

Additionally, cyber certifications can be used to match servicemembers with similar skillsets in the military, allowing them to easily transition to the civilian workforce. As transitioning servicemembers, they can also take advantage of federal government veteran hiring preferences to fill vacant cyber workforce positions at the federal level. Veterans are dedicated and talented workers that benefit any industry they work in, but unfortunately they tend to have higher unemployment rates than the general population. Since cybersecurity is a rapidly expanding field with high demand, it would be an ideal trade for veterans to work in because many have cyber experience from their military service.

The federal government faces intense competition from the private sector when recruiting highly-skilled candidates since private industry can offer much higher pay and greater career flexibility. Without the top cyber talent, we leave our nation vulnerable to intangible threats and keep government technology outdated and inefficient. To attract these workers, the federal government should establish a new national service program that forgives federal student debt within certain parameters for STEM graduates who go on to work for the federal government in cyber and information technology positions.

Developing a dynamic and expansive cyber workforce will require a large-scale approach. The cybersecurity field must be accessible to all; certifications must recognize skills and not just credentials; and the government must offer competitive and attractive opportunities for job candidates. By growing the cyber workforce and recruiting high-quality candidates to the industry, the public and private sectors will become more diverse, innovative, and secure.

Data and Information Security

Information security is paramount to a sound cyber resiliency strategy, and can be achieved in part by IT acquisition modernization and strong standard cybersecurity standards to protect personally identifiable information (PII), medical records, and information about critical infrastructure. Congress has an obligation to safeguard the PII of our constituents and sensitive national security information, while promoting new technology that can help secure our networks.

Following the passage of the Federal Information Security Modernization Act of 2014, NIST developed a Cybersecurity Framework which the federal government has been implementing in the years since. While the NIST is responsible for developing the framework and offering guidance on implementation, the Department of Homeland Security has been responsible for ensuring that each department in the federal government is implementing it properly. Within the private sector, NIST Cybersecurity Framework compliance is voluntary; however NIST has worked with industry to develop implementation guidance for the private sector, including small businesses. Despite the voluntary nature, the framework has been embraced by a wide variety of public and private sector companies with 30 percent of U.S. organizations using the framework as of 2015.

When Congressional action is necessary for security, Congress should seek to legislate based on the desired effect, not on the technology itself; policy should work in tandem with innovative technologies, not hinder them. Under this principle, we have identified several policies and proposals to address data security:

- ***Continue strict implementation of the Federal Information Technology Acquisition Reform Act (FITARA).***
- ***Continue commitment to sustained IT modernization in federal, state, and local government through partnerships with industry and a government-wide IT modernization working capital fund to incentivize agencies to save money and retire legacy IT.***
- ***Reform the Federal Risk and Authorization Management Program (FedRAMP) to serve as a model of standardized security certification processes for government IT acquisition.***
- ***Encourage stronger cybersecurity practices in the private sector, and establish a loan guarantee program for small businesses to purchase cybersecurity technology and services at no additional cost to the taxpayer***
- ***Standardize breach notification laws at the federal level.***
- ***Adopt privacy-enhancing, user-friendly, and cost-effective digital identity verification techniques that can be used in both the public and private sectors.***

The federal government spends nearly 75 percent of its IT budget on legacy systems, which are expensive to update and ill-equipped to respond to modern cyber threats. The government cannot demand high standards from the private sector, while it runs systems so out-of-date they can no longer receive vital security updates. The federal government must continue strict implementation of FITARA, modernize its IT systems, and build strong security measures into any acquisition process. Programs such as FedRAMP provide a standardized approach to certifying cloud services for the government and should be further reformed to serve as a model for other types of technology acquisition. We must continue to empower and resource federal Chief Information Officers to make the acquisitions decisions necessary to upgrade and secure federal IT.

Maintaining updated, modern technology and investing in stronger cyber defense is critical in both the public and private sectors, but the upfront investment can often be too burdensome for smaller business. The federal government could establish a loan guarantee program for small businesses to purchase cybersecurity technology and services at no additional cost to the taxpayer. Furthermore, the NIST Cybersecurity Framework should be updated to enable adoption by small businesses.

Even with prudent acquisition processes and security policy and procedures in place in the private and public sectors, systems breaches can, do, and will occur. Because breach notification laws are different in every state and requirements depend on the location of the consumer, companies have to simultaneously satisfy up to fifty-two[1] different breach notification laws. As a result, companies and organizations adopt the most strenuous laws. Companies and consumers

[1] Forty-eight states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have breach notification laws.

would benefit from standardization at the federal level. Notification laws will not necessarily affect the reasons a breach occurs, but a federal standard would help to harmonize the existing cyber regulations. To encourage stronger cybersecurity preventative measures in the private sector, the government could provide tax credits for purchasing data breach insurance for companies that comply with the NIST Cybersecurity Framework.

Individuals can be more empowered to protect their data through policies and practices that simplify identity authentication requirements and processes. Many business and government transactions require identity authentication or legally-binding electronic signatures, especially for services that require secure communication of sensitive information. However, many methods of identification require users to unnecessarily overshare sensitive PII with third parties. Personal identifiers like SSNs, Date of Birth, and Mothers' Maiden Names have been overused for means of "access." By linking identifiers to access, SSNs are now a commodity for cybercriminals. A shift away from this model needs to happen quickly and new innovative solutions must be implemented in the market. Similarly, the widespread practice of maintaining dozens of usernames and passwords is not an effective, long-term method for keeping data secure. We support both government and commercial adoption of privacy-enhancing, user-friendly, and cost-effective digital identity verification techniques. Participation in these identity systems should be completely voluntary and be driven by market-interest. Government agencies, such as NIST, have a role to play in crafting standards for these identity authentication systems.

Ultimately, modernizing and simplifying certain aspects of technology acquisition, raising federal- and industry-level standards and strengthening individual data privacy can protect the government, companies, and consumers from information breaches.

Internet of Things (IoT)

The growth of the Internet of Things (IoT)—the network of Internet-connected everyday objects that can process, send, and receive data—reflects the fact that the Internet is present in nearly every aspect of the modern world, creating an extensively interconnected environment. These devices have made tangible improvements to people's lives, improving health and safety, quality of life, and personal savings. Smart materials alert us to cracks and faulty structures in bridges, thermostats adjust temperatures before homeowners return, and body monitoring devices track blood glucose levels for diabetics. Yet many of these devices lack basic security features, like identity authentication, and cannot receive critical security updates. There are a few simple solutions that address these concerns:

- ***Ensure that IoT devices are designed to be secure out of the box and with the ability to secure the device over a network, or through automated or unattended means and clearly inform consumers about this functionality.***
- ***Direct the federal government to partner with the private sector to create and distribute cyber hygiene public service announcements (PSAs).***
- ***Develop definitions to categorize IoT devices to allow for appropriate application of security standards, best practices and compliance with current industry specific regulations.***

People use IoT devices for ease and convenience, but these connected devices can make users more vulnerable by creating multiple points of entry for a cyberattack. We need to encourage security by design so these devices are able to receive live patch updates and better protect their users. Industry and government must work together to incentivize higher security standards to combat these kinds of vulnerabilities.

To better educate the public about cybersecurity and any vulnerabilities, the federal government should partner with the private sector to create and distribute public service announcements targeted at improving cyber hygiene. Devices are only as secure as the people who use them and improving the practices of individual users is a critical step toward increasing security. These projects should:

- Provide simple steps for improving security, such as changing default Wi-Fi passwords.
- Communicate the risks of phishing and other common tactics used to exploit users.
- Explain how to easily recognize suspicious or threatening online activity.
- Give the public information about how best to respond when victimized by cyberattacks.

The government has a valuable opportunity to lead in this space by leveraging its convening authority. We need to bring together relevant stakeholders to discuss the best ways to define and characterize IoT devices and develop standardized, comprehensive security practices for these devices. Doing so will help frame the approach that government entities and industry stakeholders take in developing everything from hardware and software to technology standards and updated laws.

Conclusion

Everyone has a role to play in improving the cyber ecosystem—whether it is federal, state, and local governments, industry, or individuals—and the most effective policy solutions will be those that leverage the input, innovation, and partnership of the public and private sectors. The Task Force is prepared to actively work with the Executive branch, industry, and other stakeholders to make sure we are coordinating and communicating a strategy forward. Our interconnected world requires an active, agile, and resilient approach and there is no time to waste in developing our defense and response infrastructure. Properly addressing the threat of cyberattacks will not only bolster security, but will create new industries and jobs and boost our economy. It is both an exciting and formidable responsibility; we can take advantage of this moment if we constructively work together.

For any of these policies in the United States to be truly effective, we must work with the international community. The nature of technology and the Internet is global: our businesses routinely conduct digital trade; our students collaborate with researchers across the world; and we have more access to the ideas and entertainment of other cultures than ever before. Yet the cybersecurity standards and legal and enforcement apparatuses of those countries may not necessarily be on par with our own. We must engage the international community to establish and expand global cybersecurity standards to protect business, institutions, and individuals, no matter where they live or operate.

The New Democrat Coalition Cybersecurity Task Force has already begun taking important steps toward addressing our cybersecurity challenges. We have written multiple letters to the Trump administration encouraging both smart investments in cybersecurity as well as updated cyber workforce hiring practices. The Task Force is evaluating the best course of action to achieve the above-mentioned policy objectives, whether through legislative processes, by working with the Executive branch, or partnering with industry. We hope that public and private sector leaders see us as willing partners to tackle these challenging problems, and we look forward to continuing our work in cybersecurity policy.