Cybersecurity Framework for Improving Critical Infrastructure

What Others are Saying

Table of Contents

Energy Companies

- **Joseph Rigby, Chairman and CEO, Pepco Holdings Incorporated:**
  "We believe the partnership between the government and affected industries is critical to ensure preparation and readiness; this Framework is evidence of the commitment of stakeholders to work together to protect against cyber threats."

- **Bennett Gaines, Senior Vice President, Corporate Services and CIO, FirstEnergy:**
  "The secure and reliable operation of our transmission infrastructure is a responsibility we take very seriously at FirstEnergy. We believe the NIST cyber security framework provides a workable approach to protecting our bulk transmission system and are pleased to have been part of the development effort. We look forward to continuing to work with the federal government, our peers in the electric industry and other stakeholders to advance our capabilities to protect our assets through collaboration."

- **Leo Staples, Senior Manager Utility Operational Compliance, Oklahoma Gas & Electric:**
  "OGE Energy Corp. is committed to protecting the Nation's electric grid as a part of our commitment to providing reliable service to our customers. We believe the recently released Framework developed by NIST is an important consideration when determining how best to protect the Nation's critical infrastructure. We look forward to utilizing the NIST Framework as a part of the paradigm from which we form the basis of our Integrated Security Plan."

Financial Service Companies

- **Charles W Scharf, CEO, Visa:**
  "Visa supports a standards-based approach, and we're encouraged by the final framework issued by the Administration which promotes the adoption of existing security best practices. We also support robust information sharing programs with appropriate liability protections to further bolster global cyber security."

- **Michael Bodson, President and Chief Executive Officer, DTCC:**
  "The NIST Cybersecurity Framework represents a milestone achievement. It is the result of a year-long public-private partnership, which is vital to the financial services industry's cybersecurity ecosystem and plays a key role in our sector's ability to identify threats, respond to cyber incidents and coordinate with government partners. The Depository Trust & Clearing Corporation (DTCC) was pleased to work with the Administration and the industry to help develop these voluntary guidelines and looks forward to leveraging the Framework as a means to help reduce cyber risks to critical infrastructure. Given the systemic impact cyber security threats could have on the financial industry, the Framework is a key step in protecting the nation."

Telecommunications Companies

- **Larissa Herda, Chairman and CEO, tw telecom:**
  "We applaud the White House for bringing government and industry together to create the Cybersecurity framework. Establishing a framework of best practices and standards is an important step toward improving our country's critical infrastructure and security posture. We hope that all businesses will look to this framework, as we do, to strengthen their cybersecurity practices. It is in the best interests of our country to do so."

- **Edward Amoroso, Senior Vice President and Chief Security Officer, AT&T Services:**
  "AT&T applauds the National Institute of Standards and Technologies on the release of its Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. While we will be reviewing the details of the Cybersecurity Framework over the coming months to see how it best complements our existing cyber-risk management program, a few things are clear now: First, the Cybersecurity Framework builds upon existing industry security standards and spans all 16 sectors of critical infrastructure. Effective cybersecurity presents a complex challenge requiring collaboration from across the entire Internet ecosystem. Second, the Cybersecurity Framework builds in the necessary flexibility for effective implementation and continued innovation. This flexibility is vital, as it allows organizations to adapt and evolve as the threat landscape continuously shifts. Third, the Cybersecurity Framework shows international leadership by demonstrating that an effective partnership between government and industry is the most effective way to combat cyber-attacks. In that spirit, later today, our CEO, Randall Stephenson, will participate in a roundtable discussion at the White House with Secretary Pritzker and other industry leaders on the Cybersecurity Framework. We look forward to continuing

our work with government and industry partners to effectively protect the nation's critical infrastructure from existing and future cybersecurity threats."

- **Craig Silliman, Senior Vice President, Public Policy, Verizon:**
  "Verizon has long focused on protecting the security and privacy of our customers, as well as protecting our networks. All businesses – large and small – need to keep their cyber security defenses updated to respond to continually evolving cyber threats, but not all businesses have the tools or resources to do so. We applaud the Administration for bringing together a wide range of stakeholders to create this Framework, which provides a useful tool for companies as they consider the right mix of cyber defenses to protect themselves and their customers."

- **Steve Davis, Executive Vice President for Public Policy and Government Relations, CenturyLink:**
  "CenturyLink commends NIST on the release of its national cybersecurity framework. This framework provides a common language and is the necessary first step in improving communications among government and industry stakeholders. We applaud NIST for partnering with the private sector during this year-long endeavor and believe the framework will serve as a solid foundation for continued collaboration that will enhance our nation's overall cybersecurity posture."

- **Myrna Soto, Senior Vice President and Chief Information & Infrastructure Security Officer, Comcast Cable:**
  "Comcast commends the White House for its commitment to an industry-collaborative process and for its recognition that a flexible, voluntary framework, rather than prescriptive regulation, is the best means of strengthening our overall cyber defense posture. The Cybersecurity Framework represents a comprehensive compendium of sound and effective cyber defense processes, practices, and protocols available today. We will evaluate the Framework Core to assess whether it can be tailored and adapted to our business circumstances and network configuration, and possibly serve as a reference tool for managing the cyber risks and threats we face."

- **Brian Allen, Group Vice President and Chief Security Officer, Time Warner Cable:**
  "Cybersecurity is a high priority for us, and we devote significant attention and resources to ensure that our networks and our customers' information are safe. We appreciate the collaborative process established by NIST and efforts to ensure that the Cybersecurity Framework promotes innovation, and is flexible and adaptable. We look forward to reviewing the Cybersecurity Framework and continuing to work with NIST, the Department of Homeland Security and others on this critical issue."

Information Technology Companies

- **Renee James, President, Intel:**
  "Improving cybersecurity in ways that promote innovation and protect citizens' privacy is the only way to preserve the promise of the Internet as a driver of global economic development and social interaction. Intel applauds the Administration and the National

Institute of Standards and Technology for constructing the cybersecurity framework hand-in-hand with industry and other stakeholders, building a model of a voluntary, risk-based tool that can be utilized by a broad array of organizations. We look forward to further work together to help the framework gain traction and see cybersecurity practices elevated around the world."

- **Mark McLaughlin, Chief Executive Officer of Palo Alto Networks:**
  "Palo Alto Networks is dedicated to helping organizations achieve the highest possible degree of cybersecurity across all networks and infrastructures. The cross-sector harmonization reflected in the Framework is a positive step to creating and sharing best practices across industry, and between industry and government. Cybersecurity is a shared concern of the greatest urgency and seriousness and the Framework is helpful in focusing these efforts."

- **Steve Bennett, President & CEO, Symantec Corporation:**
  "The effort to develop the NIST Cybersecurity Framework has been a model of public-private partnership. Symantec believes the Framework will be useful to all organizations, whether they have well-developed cybersecurity programs or are looking to start one. It was essential that the Framework be industry-driven and reflect existing, accepted standards and practices – and NIST accomplished that. Symantec has already begun to incorporate the Framework into our internal security program, and I expect that many of our customers will use it as well."

- **Kristin Lovejoy, General Manager, IBM Security Services:**
  "IBM congratulates NIST on the release of the Cybersecurity Framework and strongly supports its voluntary, flexible and risk-based approach. The Framework addresses key security issues for today's critical infrastructure companies - and can be adapted by organizations of all types and sizes as a valuable tool to improve their cybersecurity posture. IBM plans to help our clients implement the Framework as part of their own cybersecurity risk management programs - news we'll share in the coming days. We look forward to continuing our partnership with government and industry on the Executive Order and future versions of the Framework."

- **Scott Charney, Corporate Vice President, Microsoft, Trustworthy Computing Group:**
  "Microsoft welcomes the release of the Cybersecurity Framework, an important milestone in national efforts to improve the security of critical infrastructures. The Framework helps advance security and privacy by providing flexible guidance for cybersecurity risk management, focusing on what organizations should do without being overly prescriptive as to how they do it, and promoting international standards and industry best practices. Microsoft commends NIST for its collaborative approach to developing the Framework. The transparent and inclusive process used by NIST provides a template for how industry and government should work together on cybersecurity and privacy. Microsoft's approach to managing cybersecurity risks is consistent with the Cybersecurity Framework's security and privacy guidance. The Framework seeks to foster a culture of risk management, similar to the culture driven by

Microsoft's policies and practices that involve regular assessment of the security and privacy challenges facing our customers and our operations, as well as ongoing application of learnings gained through our experiences defending over one billion users from cyber-threats. We look forward to continuing our work with NIST and others in industry to advance risk-based initiatives like the Cybersecurity Framework."

- **Justin Somaini, Chief Trust Officer, Box:**
  "The rapidly evolving nature of cybersecurity threats today demands close partnerships both among industry players and between industry and government. Advancements like the Cybersecurity Framework are important steps towards identifying and promoting the broad adoption of best practices and technology that we need to ensure a secure and productive society. Security and privacy are fundamental to Box's business, and we wholeheartedly support the Framework's objectives."

- **Suzanne Magee, CEO, TechGuard Security:**
  "The development of a voluntary framework is a critical step towards measuring the progress that is being made to protect our critical assets. I applaud NIST and the Administration on the release of this framework."

- **Philippe Courtot, CEO, Qualys:**
  "Attacks continue to escalate, cyber threats remain dangerous. It is essential that the government and private sector work in partnership to protect our national critical assets. Today's release of the NIST voluntary framework takes that important next step"

- **Steve Orenberg, President Kaspersky Lab, North America:**
  "The Cyber Secure America Coalition appreciates the collaborative effort by NIST to develop the voluntary cyber framework for critical infrastructure. This was an inclusive effort with the private sector and key experts resulting in a solid document and reference for the critical infrastructure."

- **Felix Sterling, General Counsel, TrendMicro:**
  "The risk based approach to the NIST framework target profiles will ensure appropriate deployment of resources and will permit continued innovation to stay ahead of the bad guys."

- **Phil Dunkelberger, CEO, Nok Nok Labs:**
  "Cyber threats are real and continue to escalate. I applaud the successful release of the NIST voluntary framework. This document and future efforts by NIST and security experts will serve as a key guide to make our national critical infrastructure more secure."

Industrial Control System Companies

- **Keith Nosbusch, Chairman and CEO, Rockwell Automation:**
  "Rockwell Automation is honored to have actively contributed to the development of the Cybersecurity Framework that will help address cyber risks to critical infrastructure and manufacturing processes alike. This guideline provides a flexible structure that can help

organizations improve information security protection programs to manage risks to industrial control and information systems using the Connected Enterprise."

- **Doug Wylie, Director, Product Security Risk Management, Rockwell Automation:**
  "As the world's largest company dedicated to providing industrial automation solutions, Rockwell Automation strongly supports this voluntary Cybersecurity Framework because it helps to amplify the importance of protecting national critical infrastructures and related industrial control systems that operate tirelessly to provide reliable power, clean water, safe food and to keep other key manufacturing processes running safely and efficiently."

- **Greg Scheu, President and CEO, ABB Inc.:**
  "We believe the cybersecurity framework is an important step forward and applaud its direction. It recognizes the need for a strong public-private partnership and effective information sharing. It lays out an approach for industry and infrastructure providers to assess the maturity of their cybersecurity program. Even more, the framework makes clear this will be an ongoing, evolutionary process."

- **Raj Batra, President, Siemens US Industry Automation:**
  "The Cybersecurity Framework gives leaders at the organizations that own critical infrastructure a core set of productive questions to ask themselves, the managers who report to them, and their business partners about security. As a global supplier of industrial control systems and managed services for cybersecurity, we appreciate the Framework's clear references to existing, international, consensus-based security standards."

- **Michael Caliel, President and CEO, Invensys:**
  "Cyber security and cyber threats are an ever-more complicated challenge for American industry as its equipment and infrastructure continue to age. As companies seek to strengthen and modernize their control and safety systems, they need to take a more holistic view of their cyber security requirements. Modern systems, intrusion prevention, firewalls and other cyber technologies are important, but comprehensive cyber protection frequently involves changing the company culture. This new framework is a great first step on that journey-- a starting point on the road to a more secure critical infrastructure-- because it can help individual plant operators and other personnel learn to identify vulnerabilities and then rely on standards-based best practices and solutions to mitigate risks. With enough momentum, we believe it will help improve the security posture of industrial control systems everywhere."

Health Care Companies

- **Terry Rice, CISO, Merck & Co, Inc:**
  "Merck has begun adoption and implementation of the Cybersecurity Framework…. Merck commends NIST's superior leadership in advancing the foundation of cybersecurity through this new Framework and looks forward to continued evolution and

expanded adoption within the Health and Public Health sector. Congratulations on a job well done."

Insurance Companies

- **Peter J. Beshar, Executive Vice President and General Counsel, Marsh & McLennan Companies, Inc.:**
  "Cyber security is an evolving threat. The Administration's Framework is an important tool to help the private sector improve its readiness and resilience."

Defense Companies

- **Marilyn Hewson, Chairman, President and CEO, Lockheed Martin:**
  "Cybersecurity is a shared responsibility between government and industry, and we applaud the Administration for making it a priority. We support the Administration's voluntary, transparent and flexible approach to developing the Cybersecurity Framework, and believe it will enable American businesses—large and small—to do their part."

Security Consulting Companies

- **Michael Chertoff, Secretary of Homeland Security under President George W. Bush and Chairman of the Chertoff Group:**
  "The release of the Cybersecurity Framework is a helpful step forward in providing guidance and best practices to help companies, particularly small and medium sized companies, grappling with today's cyber threats."

- **Paul Kurtz, Chief Strategy Officer, CyberPoint International:**
  "CyberPoint commends NIST's work to consolidate guidance and standards into a common framework. It is an important step forward in helping the cyber security marketplace and the critical infrastructure sector work together for a more secure future."

- **Wall Street Journal CIO Network Task Force on Cybersecurity:**
  "Recommendation 1. Adopt NIST Standards. U.S. companies and institutions should work with the government to adopt the pending National Institute of Standards and Technology cybersecurity framework."

Trade Associations

- **Dean C. Garfield, President & CEO, Information Technology Industry Council (ITI):**
  "The NIST Framework is a model example of the public and private sectors working together effectively to serve the national interest. We have a shared interest in strengthening the nation's cybersecurity and the Framework moves us significantly towards that goal. The Framework represents an effective approach to cybersecurity because it leverages public-private partnerships, is based on risk management, is voluntary, and points to globally recognized, consensus-based standards and best

practices. Both the private sector and government have important roles to play in improving cybersecurity, and the tech sector was pleased to have worked closely with NIST and other stakeholders to develop this Framework. ITI looks forward to continuing to work with the Administration and Congress on additional steps we can take to improve cybersecurity."

- **Tim Pawlenty, CEO, Financial Services Roundtable:**
  "FSR applauds NIST's Framework and we were proud to have been involved in this important effort. We were pleased to see NIST included our priorities around robust privacy protections for consumers. We look forward to working with Congress on cyber threat information sharing to ensure our industry's customers are ultimately protected."

- **Walter B. McCormick Jr, President & CEO, US Telecom:**
  "US Telecom congratulates NIST's work on creating the 2014 Cybersecurity Framework which provides an approach for industry to identify and evaluate best practices for improving the security of critical infrastructure. The framework emphasizes a multi-stakeholder, voluntary, flexible and cost-effective approach that can be used by organizations of all types and sizes to assess and address their unique risk circumstances, and develop solutions that best fit each organization. We encourage NIST to continue to provide leadership in the cybersecurity arena for the benefit of all consumers who rely on a diverse ecosystem with shared responsibilities."

- **Frank Keating, President and CEO, American Banking Association:**
  "We welcome the cybersecurity framework issued today by the National Institute of Standards and Technology as directed by the Obama Administration. The framework reflects existing regulations and practices within the financial services sector. It also provides important direction to the public sector on improving cybersecurity soundness and ultimately the safety of our nation's critical infrastructure. Banks and other financial services companies have made cybersecurity a top priority and are subject to the most stringent regulatory requirements. We have put in place the highest level of security among critical sectors, and become a role model sector for cooperation, effectiveness and security. We look forward to continuing to work with the Financial Services Sector Coordinating Council, the administration and Congress toward our mutual goal of protecting our nation's critical assets."

- **Angela Gleason, Associate Counsel, American Insurance Association (AIA):**
  "AIA commends NIST for its diligent and thoughtful work in the development of the Framework and we appreciated the opportunity to provide input during the development process. We look forward to seeing the potential impact the Framework may have on the nation's cyber resiliency. The White House and Department of Homeland Security (DHS) are tasked with exploring methods to implement the adoption of the Framework and have indicated they will host a number of workshops and seek public comment through request for information on a number of topics. AIA looks forward to working with DHS as it begins to talk with insurance carriers and requests feedback from the public on how the government can help grow the cybersecurity insurance market."

- **Tim Molino, Government Relations Director, BSA:**
  "This framework creates the conditions for a productive public-private partnership that will bolster cybersecurity while promoting innovation. NIST has solicited input from industry and other public stakeholders to ensure the framework leverages and promotes best practices on a voluntary basis. This approach acknowledges there are no silver bullet solutions to enhance cybersecurity. What we need instead is an ongoing process of innovation and adaptation to counter the evolving threat environment. It is a long journey, but we're heading in the right direction."

- **Jim Linn, Managing Director, Information Technology, American Gas Association:**
  "AGA leadership and members have participated in all five NIST Cybersecurity Framework workshops and have submitted consensus industry comments during each request for formal comments during the development process. We see the framework as a means to identify areas for improvement of critical infrastructure cybersecurity posture. We are also enthusiastic about the anticipated Oil and Natural Gas Cybersecurity Capability Maturity Model, a combined Department of Energy and industry-developed tool to help companies in our sector to implement the Cybersecurity Framework. We plan to encourage our members to utilize these tools to advance cybersecurity in their companies and broadly in our industry."

- **David K. Owens, Executive Vice President of Business Operations, Edison Electric Institute:**
  "Providing safe, reliable electricity is the electric power industry's top priority, and we are focused on actions to enhance the security and resiliency of the grid. The industry appreciates the Administration's efforts to develop the NIST framework and its willingness to allow our companies to provide input. This collaborative effort between the public and private sectors is yet another example of the strong industry-government partnership that has developed to enhance the protection of our nation's critical infrastructure assets. We look forward to continuing to collaborate with the government on the implementation of the framework to align it with existing and ongoing cybersecurity investments."

- **James Assey, Executive Vice President, National Cable & Telecommunications Association:**
  "The cable industry appreciates the collaborative process between the National Institute of Standards and Technology and industry in the development of the Cybersecurity Framework. Now that the final framework has been released, we will review the document and continue to work with the Department of Homeland Security and other relevant parties toward the further development of a Voluntary Program that will improve cybersecurity."

- **W. Hord Tipton, CISSP, Executive Director (ISC)^2:**
  "As the global leader for inspiring a safe and secure cyber world, (ISC)^2 applauds the actions by NIST to develop a voluntary framework to identify cybersecurity risks. This framework reemphasizes the growing need for businesses to demand qualified

information security professionals with the skills and knowledge to create, understand, and implement such programs."

- **Phil Bond, Executive Director, Cyber Secure America Coalition:**
"The NIST Framework is good news for anybody that wants to see U.S. networks more secure. Not only will it improve the cyber security of the national critical infrastructure, it also could create the environment for rapid deployment of market-based incentives for all commercial interests to start taking security seriously. The Cyber Secure America Coalition is pleased with the progress made to date and looks forward to continuing a productive effort in partnership with NIST to make our nation more cyber secure."

Civil Society and Privacy Groups

- **Michelle Richardson, Legislative Counsel, American Civil Liberties Union:**
"Integrating privacy and civil liberties principles into emerging cybersecurity programs is necessary to ensure that legitimate security efforts don't morph into surveillance or censorship programs. We appreciate the Administration's commitment to the Fair Information Practice Principles and hope to work with companies to make these voluntary standards a part of their daily business."

- **Greg Nojeim, Director of the Project on Freedom, Security & Technology, Center for Democracy & Technology:**
"The framework provides a number of cybersecurity guideposts for the companies that choose to implement it. More work needs to be done to create more and clearer privacy guideposts that go beyond recommending that privacy processes be in place, the framework is a start that will help the privacy officers in the companies that adopt it push for meaningful privacy practices."

- **Ginny Sloan, President, The Constitution Project:**
"Effective cybersecurity is not possible without robust privacy protections. While we believe that Fair Information Practice Principles will need to play a larger role in future versions of the Framework, we recognize that setting out a process for considering privacy measures is a significant first step toward putting protections in place. We appreciate NIST's openness and inclusiveness throughout the development of the Framework. And we look forward to ongoing discussions with industry leaders as we identify and promote best practices."

- **Terry Ives, Chair, Automation Federation:**
"The risk of cyberattacks targeted to industrial automation and control systems across all industry sectors continues to grow. The Cybersecurity Framework provides a more comprehensive approach for industry sectors to determine their vulnerability to these kinds of attacks and the means to mitigate them."

Congress

- **Senator Charles Grassley (R-IA), Ranking Member of the Committee on the Judiciary:**
  "The government has a strong interest to work together with industry, given the impact cyber-attacks have on the nation's economy. Fostering a greater public-private approach to cybersecurity was recognized in last year's Executive Order from the President on Improving Critical Infrastructure Cybersecurity. The Executive Order stated that strengthening cybersecurity can be achieved through government partnership with private business. As a result of the Executive Order, we should review the National Institute of Standards and Technology ongoing partnership with owners of critical infrastructure. This partnership will create standards, guidelines, and best practices for businesses to implement on a voluntary basis. There's already bipartisan support for this approach."

- **Senator Jay Rockefeller (D-WV), Chair of the Committee on Commerce, Science, and Transportation:**
  "The recent data breaches at Target and other retailers are a stark reminder that our networks continue to be vulnerable to cyber attacks. The Cybersecurity Framework NIST released today represents a major step forward in improving our cyber defenses. This Framework represents the careful thinking of our country's top security experts. It should become an essential touchstone, not just for critical infrastructure operators, but for all companies and government agencies that need to protect their systems and their data. I congratulate NIST and President Obama for bringing the public and private sectors together to develop this important new cybersecurity tool."

- **Senator Barbara A. Mikulski (D-MD), Chairwoman of the Appropriations Committee:**
  "Consumers depend on the companies they buy from and bank with to keep scammers and thieves out of their wallets. The NIST Framework for Cybersecurity released today can help businesses improve cybersecurity and protect consumers. This Framework represents NIST and industry working together to develop cybersecurity best practices that keep Americans safer and our economy stronger."

- **Senator Tom Carper (D-DE), Chairman of the Committee on Homeland Security and Governmental Affairs:**
  "This voluntary framework provides a much needed roadmap for improving the cybersecurity of our most critical infrastructure. I appreciate the dedicated efforts of those from industry and the federal government who worked diligently together to develop it over the last year. Companies now have a common, but flexible path forward to better secure their systems, and also a meaningful way to measure their progress. We must now focus like a laser on ensuring widespread implementation of the framework in order to effectively protect our national and economic security."

- **Senator Tom Coburn (R-OK), Ranking Member of the Committee on Homeland Security and Governmental Affairs:**
  "What we have to do is what's in the best interest of the nation, and I think the president

has shown real leadership with this executive order."

- **Senator John Thune (R-SD), Ranging Member on Commerce Commerce, Science, and Transportation:**
  "I applaud the work NIST has done over the past year to solicit input from private sector partners to address the growing cybersecurity threat. As we move forward, the NIST framework should remain voluntary and industry-led, as outlined in the bill Chairman Rockefeller and I introduced last year, which was approved by the Senate Commerce Committee in July. Congress also needs to work to ensure that information about cyber threats – like the malware behind recent attacks on retailers – can be shared quickly and effectively, while safeguarding privacy and civil liberties."

- **Senator Sheldon Whitehouse (D-RI), Chair of the Judiciary Subcommittee on Crime and Terrorism:**
  "The framework released today by the Obama Administration is an important step toward protecting critical infrastructure from cyber attacks. While Congress must ultimately take action to complement this framework, it's important for the Administration and the private sector to continue making progress to protect our communities. That's exactly what this framework will do."

- **Representative Bennie G. Thompson (D-MS), Ranking Member, Committee on Homeland Security:**
  "I am pleased that the NIST framework, outlined in the President's cybersecurity executive order, is now complete and on time. The framework will help secure the nation's critical infrastructure from cyber attacks by cultivating a valuable partnership between the government and the private sector. Establishment of the cyber framework is a positive step forward, reinforced by the new DHS voluntary program intended to promote broad use of the NIST cybersecurity best practices."

- **Representative Jim Langevin (D-RI), Co-Chair of the Congressional Cybersecurity Caucus:**
  "I commend the Administration, the National Institute of Standards and Technologies, and participating stakeholders from across academia and industry for their development of the Cybersecurity Framework. The Framework's flexible approach will help owners and operators to better safeguard vulnerable critical infrastructure while protecting privacy and civil liberties. With the continued failure of Congress to enact comprehensive cybersecurity legislation, the need for executive action could not have been more clear, and the release of the Framework is only the most recent illustration of the Administration's commitment to defend our nation in cyberspace. I hope that Congress will use the release of the Framework as the impetus to swiftly consider and enact legislation that builds upon the Administration's efforts in order to make meaningful and wide-ranging improvements to our cyber defenses."

- **Representative Michael McCaul (R-TX), Chairman of the Committee on Homeland Security:**
  "The *National Cybersecurity and Critical Infrastructure Protection Act of 2013*, which

passed the Homeland Security Committee unanimously, supports both DHS's and NIST's role in collaborating with the private sector to address cyber vulnerabilities and to raise the bar on cybersecurity. While our bill differs from the Executive Order, we can agree that the public-private partnership to protect critical infrastructure must be strengthened. We look forward to working with both the Senate and the Administration to get legislation to the President's desk that will further protect our Nation's critical infrastructure such as our banking, gas pipelines, and water systems from Iranian, Russian, and Chinese hackers who seek to harm our way of life."

State and Local

- **Virginia Governor Terry McAuliffe:**
  "Adding this framework to the existing efforts led by the Secretary of Technology, Chief Information Officer, Chief Information Security Officer and the Virginia Information Technologies Agency will strengthen the Commonwealth's ability to fight cyber crime and further enhance Virginia's position as a leader in cybersecurity. Virginia has an award-winning cybersecurity program in place, but must continue to advance our ability to keep our families and businesses safe and make the Commonwealth the national hub for the cybersecurity industry and the jobs that come with it."

- **Michigan Governor Rick Snyder:**
  "As a global leader in government cybersecurity, Michigan applauds the efforts of the National Institute of Standards and Technology and this resulting framework. It's a critical step forward in strengthening our nation's cyber defenses. It establishes best practices that will be used across the public and private sectors, enhancing our country's ability to defend against and recover from cyber attacks. We appreciate the significant work that went into this initiative and view it as an excellent platform for further collaboration that leads to our shared goal of a safer America. It is a proactive, comprehensive approach to preventing, detecting, responding, and recovering from cyber incidents."

- **Doug Robinson, Executive Director, National Association of State Chief Information Officers:**
  "NASCIO believes the cybersecurity framework is an excellent way to approach the fundamentals of cybersecurity. It will provide a foundation upon which the public sector can build greater protection against cyber threats and collaborative cybersecurity partnerships among all levels of government. NASCIO appreciated the continuous outreach from federal stakeholders in developing the Cybersecurity Framework, and looks forward to continuing our partnership to secure public sector data and infrastructure."