ESPC
Email Sender & Provider Coalition

MEMORANDUM

To: **ESPC Legislative Committee and ESPC Security Tech Committee**

Cc: **ESPC Board**

From: Reed Freeman
Jonathan Cedarbaum
WilmerHale

Re: **Presidential Cybersecurity Commission Issues Ambitious Policy Roadmap for Next Administration**

On Thursday, December 1, the nonpartisan Commission on Enhancing National Cybersecurity, established pursuant to an Executive Order in February, issued its report, outlining more than 50 recommendations for the next Administration. Among the most striking are calls for:

- regulatory agencies to "harmonize existing and future regulations with the National Institute of Standards and Technology (NIST) Cybersecurity Framework to focus on risk management—reducing industry's cost of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation";

- the federal government to "extend additional incentives to companies that have implemented cyber risk management principles and demonstrate collaborative engagement";

- development by a private body of "the equivalent of a cybersecurity "nutritional label" for technology products and services—ideally linked to a rating system of understandable, impartial, third-party assessment that consumers will intuitively trust and understand";

- creation by Executive Order of a "National Cybersecurity Private–Public Program (NCP3) as a forum for addressing cybersecurity issues through a high-level, joint public-private collaboration";

- establishment of a Cybersecurity Framework Metrics Working Group (CFMWG) to develop industry-led, consensus-based metrics that may be used by (1) industry to voluntarily assess relative corporate risk, (2) the Department of Treasury and insurers to understand insurance coverage needs and standardize premiums, and (3) DHS to implement a nationwide voluntary incident reporting program for identifying cybersecurity gaps, including a cyber incident data and analysis repository (CIDAR);

- rapid development, under NIST's leadership, working with industry and voluntary standards organizations, of a comprehensive set of risk-based security standards for Internet of Things (IoT) devices and systems;

- launching of a "national public–private initiative to achieve major security and privacy improvements by increasing the use of strong authentication to improve identity management";

- recognition that the federal government "is—and should remain—the only organization with the responsibility and, in most cases, the capacity to effectively respond to large-scale malicious or harmful activity in cyberspace caused by nation-states, although often with the assistance of and in coordination with the private sector";

- appointment by the President of an Assistant to the President for Cybersecurity and an Ambassador for Cybersecurity to coordinate U.S. cybersecurity policy domestically and abroad.

Establishment and Key Themes

Established pursuant to an Executive Order issued by President Obama in February 2016, the Commission consisted of 12 members selected in part by congressional leaders and in part by the President.[i] With the Trump Administration's appointments to many positions likely to shape its cybersecurity policies not yet determined and thus the direction of the new Administration's cybersecurity policies, unclear, it remains uncertain how influential the Commission's recommendations will be. But the Commissioners, drawn from government, business, academia, and the military, represent a knowledgeable and bipartisan group of advisers, so some of their recommendations are likely to be pursued by the new Administration.

Among the themes cutting across the report's findings and recommendations are: the ever-increasing importance of cybersecurity with the movement of more and more of our economic and other activities to the digital domain; the explosion of the Internet of Things"—devices used in all aspects of business and personal life that are connected to the Internet—and the resulting need for the development of security standards for this vast ecosystem; the urgent need for improved methods of authentication; the centrality of human factors in influencing data security vulnerabilities and solutions; and the superiority of incentives and public-private collaboration over government-mandated requirements.

Findings, Imperatives, Recommendations, Action Items

The Commission's report groups its 16 recommendations and 53 "action items" under six imperatives: (1) protect, defend, and secure today's information infrastructure; and digital networks; (2) innovate and accelerate investment for the security and growth of digital networks and the digital economy; (3) prepare consumers to thrive in a digital age; (4) build cybersecurity workforce capabilities; (5) better equip government to function effectively and securely in the digital age; (6) ensure an open, fair, competitive, and secure global digital economy. The report offers nine broad findings and ten foundational principles that drive its recommendations.

The findings are:

- Technology companies are under significant market pressure to innovate and move to market quickly, often at the expense of cybersecurity.
- Organizations and their employees require flexible and mobile working environments.
- Many organizations and individuals still fail to do the basics.
- Both offense and defense adopt the same innovations.
- The attacker has the advantage.
- Technological complexity creates vulnerabilities.
- Interdependencies and supply chain risks abound.
- Governments are as operationally dependent on cyberspace as the private sector is.
- Trust is fundamental.

The Commission's ten foundational principles are:

1. The growing convergence, interconnectedness, interdependence, and global nature of cyber and physical systems means that cybersecurity must be better managed in all contexts—international, national, organizational, and individual.

2. As the global leader for innovation, the United States must be a standard-bearer for cybersecurity. This leadership requires investing in research and collaborating with other nations, including on international cybersecurity standards.

3. The federal government has the ultimate responsibility for the nation's defense and security and has significant operational responsibilities in protecting the nation's rapidly changing critical infrastructure. The government also has cyber mission roles that need to be clarified, including better defining government (including individual agency) roles and responsibilities, and addressing missing or weak capabilities, as well as identifying and creating the capacity that is needed to perform these activities.

4. Private sector and government collaboration before, during, and after an event is essential in creating and maintaining a defensible and resilient cyber environment.

5. Responsibility, authority, capability, and accountability for cybersecurity and cyber risk management should be explicit and aligned within every enterprise's risk management and governance strategies.

6. Effective cybersecurity depends on consumer and workforce awareness, education, and engagement in protecting their digital experience. This effort must be a continuous process and advance individuals' understanding and capabilities as vital participants in shaping their own—and the nation's—cybersecurity. Nevertheless, to the maximum extent possible, the

burden for cybersecurity must ultimately be moved away from the end user—consumers, businesses, critical infrastructure, and others—to higher-level solutions that include greater threat deterrence, more secure products and protocols, and a safer Internet ecosystem.

7. Because human behavior and technology are intertwined and vital to cybersecurity, technologies and products should make the secure action easy to do and the less secure action more difficult to do.

8. Security, privacy, and trust must be primary considerations at the outset when new cyber-related technologies and policies are conceived, rather than auxiliary issues to be taken into account after they are developed. Improved privacy and trust, boosted by transparency and accountability, will contribute to the preservation of civil liberties.

9. Despite their often-constrained resources, small and medium-sized businesses are essential stakeholders in any effort to enhance cybersecurity—particularly in light of their role in the supply chain—and their needs must be better addressed.

10. The right mix of incentives must be provided, with a heavy reliance on market forces and supportive government actions, to enhance cybersecurity. Incentives should always be preferred over regulation, which should be considered only when the risks to public safety and security are material and the market cannot adequately mitigate these risks.

[i] The Commission's chair and vice chair were: Tom Donilon, former National Security Adviser to President Obama, and Samuel J. Palmisano, retired chairman and CEO of IBM. The other members were: General (Ret.) Keith B. Alexander, founder and CEO of IronNet Cybersecurity; former Director of the National Security Agency and former founding Commander of U.S. Cyber Command; Ana I. Antón, Professor and Chair of the School of Interactive Computing, Georgia Institute of Technology; Ajay Banga, President and CEO, MasterCard; Steven Chabinsky, Global Chair of Data, Privacy, and Cyber Security, White & Case; Patrick Gallagher, Chancellor, University of Pittsburgh; former Director, National Institute of Standards and Technology; Peter Lee, Corporate Vice President, Microsoft Research; Herbert Lin, Senior Research Scholar for Cyber Policy and Security, Stanford University; Heather Murren, founder, Nevada Cancer Institute; former Managing Director, Global Consumer Products Research, Merrill Lynch; Joseph Sullivan, Chief Security Officer, Uber; Maggie Wilderotter, chairman and CEO, The Grand Reserve Inn; former Executive Chairman, Frontier Communications.