Before the
United States Department of Commerce
National Institute of Standards and Technology and
National Telecommunications and Information Administration

Docket Number 130206115–3115–01

Response to Notice of Inquiry Regarding Incentives to Adopt Improved Cybersecurity Practices by Representatives of Covington & Burling LLP and The Chertoff Group

April 29, 2013

The below-listed representatives of Covington & Burling LLP and The Chertoff Group file these comments in response to the Notice of Inquiry ("NOI") on Incentives to Adopt Improved Cybersecurity Practices issued by the Department of Commerce, through the Office of the Secretary, National Institute of Standards and Technology ("NIST"), and the National Telecommunications and Information Administration dated March 28, 2013.

We appreciate the opportunity to provide comments in response to the NOI. Collectively, we have experience addressing cybersecurity issues in the government and in the private sector, including advising critical infrastructure owners and operators, as well as other companies, on their responses to cybersecurity threats. Our comments draw on our experience and propose general principles that Commerce should consider in developing incentives for participation in the Critical Infrastructure Cybersecurity Program ("the Program") contemplated in Executive Order 13,636 on Improving Critical Infrastructure Cybersecurity. These comments reflect our personal views, informed by our professional experience; they are not offered on behalf of any client of either firm or any other entity.

Cyber-based attacks implicate myriad threats to both the government and the private sector, ranging from national security compromises to economic harms caused by theft of intellectual property and financial crimes against individuals and private entities. We support the general consensus that steps must be taken to mitigate these threats. At the same time, "cybersecurity" risks should not be viewed as a unitary concept. The cyber-based risks are multiple and differentiated, and in turn, any response to such risks must be flexible enough to ensure that resources are allocated in ways that deliver the most protection to those systems, networks, and entities at greatest risk. With these concerns in mind, we suggest that Commerce consider the following principles as it structures incentives to promote participation in any cybersecurity framework developed by the government.

First, the government should ensure that whatever incentives it adopts or proposes are sufficiently flexible to account for differences in businesses and the risks they face. Those risks can vary depending on factors specific to the business, including the business's size, industry, commercial status, and status as critical or non-critical infrastructure, along with the nature of information it possesses. Even for critical infrastructure owners or operators, there may not be a "one-size-fits-all-model" with respect to the most effective and efficient way to combat cyber-

based threats. The Program—and, in turn, any incentives promoted by the government to adopt the Program—should recognize and account for these differences.

Second, on a related point, the Program or any other cybersecurity framework—and the incentives developed for participation in the framework—should take care to avoid pushing entities to comply with a static set of standards. Cyber-based threats evolve constantly, and defenses against such threats must be equally dynamic. A responsible framework—and the incentives developed to promote its adoption—should permit and encourage innovation in meeting the threats. Moreover, numerous IT-security-related regulatory and industry-led programs exist today, including, among others, the Gramm-Leach-Bliley Act (for financial institutions), the Health Insurance Portability and Accountability Act (governing protection of health records), Payment Card Industry standards (for payment card systems), and standards applied to government contractors. Many larger companies are subject to multiple IT security compliance programs. NIST should consider offering companies choice in leveraging these existing compliance regimes and companies' internal controls processes to demonstrate alignment with the cybersecurity framework.

Third, we agree with those who believe that liability protection should be considered as a way to incentivize owners and operators of critical infrastructure, as well as other entities, to participate in the Program. As demonstrated in other settings—such as the federal SAFETY Act, which provides liability protection for qualified anti-terrorism technologies—an appropriately crafted liability protection regime can provide an attractive incentive for private sector entities to achieve certain desired security practices. At the same time, some mechanism must exist to validate a company's alignment with the framework. In our view, the more predictable the validation process is, for example, in timeline, scope, and procedures, the more likely that companies will participate. Third-party, private sector-led security validation programs exist today, and the government should consider how these models might be applied to the Program.

Fourth, the incentives that NIST establishes or recommends—including liability protections—should allow for private sector entities to agree between themselves what practices and protections are appropriate to govern their obligations to each other. It is fairly common for enterprises whose systems and assets rely upon the service or connections provided by another enterprise, or who share sensitive data with another enterprise, to reach an agreement with the other enterprise about the appropriate level of security that will govern the service, interconnections, or data-sharing. These agreements are based on a variety of factors, including, importantly, each enterprise's risk assessment based on information that is only available to the enterprise. A company that has contracted with a customer to provide a certain level of cybersecurity protection should not be able to escape its contractual commitment on the ground that it meets some other standard for liability protection established to incentivize participation in the Program. Rather, incentives to participate in the Program, including liability protections, should preserve such existing contractual terms, as well as the ability of private sector participants in the Program to negotiate for cybersecurity commitments from other entities going forward.

Finally, the federal government can play a useful leadership role in incentivizing improved cybersecurity. For example, the government can incorporate cybersecurity best practices into its

procurement policies and regulations. Incorporating cybersecurity into procurement would be a low-cost, high-impact measure. It would allow companies to differentiate themselves and to compete to provide the best and most cost efficient cybersecurity protections in the products and services they provide to the federal government. The government should take care, however, that the framework and procurement regulations incorporating the framework standards are technology neutral. Technology-neutral criteria will ensure that the broadest possible range of interested companies can compete based on the cybersecurity outcomes they can deliver.

We appreciate the opportunity to share our perspective and suggestions in response to this Notice of Inquiry.

Respectfully submitted,

David N. Fagan
Kristen E. Eichensehr
Covington & Burling LLP
1201 Pennsylvania Avenue NW
Washington, DC 20004–2401
202.662.6000

Michael Chertoff*
Larry Castro
Adam Isles
Brendan Mulroy
Paul Rosenzweig
The Chertoff Group
1399 New York Avenue, NW
Suite 900
Washington, DC 20005
202.552.5280

April 29, 2013

* Michael Chertoff is the Chairman and Co-Founder of The Chertoff Group and Senior Of Counsel at Covington & Burling LLP.