Testimony of Phil Venables,

Chief Operational Risk Officer of Goldman Sachs

Before the Committee on Banking, Housing, and Urban Affairs

U.S. Senate

Chairman Crapo, Ranking Member Brown, and other members of the committee, thank you for inviting me to testify at this hearing on Cybersecurity: Risks to Financial Services Industry and Its Preparedness. I appreciate the Committee's focus on such an important issue. My name is Phil Venables; I am the Chief Operational Risk Officer of Goldman Sachs. I have been with the firm 18 years and my first 16 years at the firm I was Chief Information Security Officer before moving into a wider role in our Risk Division.

Today, I am going to provide my perspective on the cyber-threats the financial sector faces, the broader technology risk landscape, the need for shared defenses and what can be done to keep improving the security and resilience of the financial system. A number of factors are contributing to increased inherent risk across the sector including, but not limited to, the increased digitalization of financial services and the globally interconnected nature of the financial system. The same trends that are increasing benefits of a global financial system are also bringing on these new and enhanced risks.

First on threats, it will probably come as no surprise that the financial sector, globally, is targeted by a wide range of cybersecurity threats including from organized criminal groups with financial motivation as well as nation states for a broad array of reasons.

Additionally, it is worth reminding ourselves that cybersecurity is not the only risk to information or technology systems. Risks posed from software errors, misconfiguration, outages and other resiliency issues can also cause as much impact as cybersecurity events.

It is critical to have shared defenses across the financial sector so that all institutions, large and small, can learn from each other's best practices and so that threat information can be shared among firms, reducing the likelihood attackers can execute their strategies without response.

We have a long history of robust information sharing processes, with the FS-ISAC acknowledged as a preeminent example of such capability. Additionally, we have established tighter coupling between systemically important institutions through the Financial Systemic Analysis and Resilience Center, the so called FS-ARC. In addition, the sector's coordinating council under the Department of Treasury's leadership have proved instrumental in increasing sector resilience. Formalized sector-wide drills and exercises have spawned other initiatives, like Sheltered Harbor – an approach for firms to ensure the maintenance of immutable data vaults.

Turning our attention to regulators and regulation, we benefit from a number of strong regulators across the financial sector that stipulate cybersecurity and other controls that reduce the risk of major incidents. This includes regular examinations and reviews. We continue to support the need for harmonization of regulation, domestically and globally, and we commend the efforts to date on the use of the NIST Cybersecurity Framework. Additionally, we should be watchful for unintended detrimental consequences to cybersecurity from non-cybersecurity legislation or regulation.

Notwithstanding the strong relationship on this issue between the public and private sectors, we continue to examine ways to enhance coordination. For instance, there is room for improvement in the responsiveness to financial sector Requests for Information. The establishment of the DHS National Cybersecurity and Communications Integration Center (NCCIC) in 2009 created the ability to have financial sector representatives in a cleared, collaborative space working directly with partners from government and other industries for common purpose. Collaboration, engagement, responsiveness, between and among DHS, other U.S. government and industry partners continues to improve as relationships build and partners are better able to understand each other's information needs. We would propose that metrics be established between the government and financial sector to quantify and validate the flow, value and timeliness of information shared between the financial sector and public sector to quantify the state of these relationships.

Despite all this coordination and response to cybersecurity threats, risk still remains and we need to continue to be vigilant to adjust the defenses of individual firms and the sector as a whole by making sure we adopt innovative approaches to protecting customer data and services as well as designing for resilience to reduce single points of failure and single focal points of attack.

Finally, I would recommend all organizations that operate critical public services or protect customer data adopt strong defenses and security programs based on, at a minimum, the following approaches:

1. Integrate cybersecurity into the fabric of organizations – from business risk management processes, strategy and product development to the foundation of how the technology is built and operated, including planning for resilience in the face of attacks. Sustaining cybersecurity is a first class business risk along with all other risks – beginning with the Board and executive leadership and through all levels of the enterprise.

2. Improve capabilities amongst people, process and technology. There needs to be continued emphasis on the embedding of controls into critical technology products and services: we need secure products, not just security products. We should recognize that cybersecurity risk mitigation is not solely the responsibility of designated cybersecurity professionals but is, perhaps more importantly, in the domain of leadership, risk managers and engineers at all levels of organizations. I would support a national

program to embed cybersecurity training into all academic and professional training and qualifications: we need more security-minded people, not just more security people. I fully endorse efforts to deal with the shortage of trained cybersecurity professionals to help manage these risks, but I also note that there is a wider issue related to the productivity of the cybersecurity professionals we already have and more needs to be done by government and industry to improve tools, processes and the orchestration of defense across multiple platforms to get the most out of those people.

3. Design for defensibility. Our goal should be to design our technology and information processing environments to be more inherently defendable and resilient in the face of attacks, and we have to keep examining our global supply chains for security issues and excess concentration risk on specific services or geographies.

Thank you again Mr. Chairman for allowing me to provide this input into this important process and we remain committed to assisting further as needed. I'm happy to answer any questions you or the other members may have at this time.