Written Testimony of

Mr. Mark Clancy, Managing Director, The Depository Trust & Clearing Corporation

On behalf of the

American Bankers Association, Financial Services Roundtable, and

Securities Industry Financial Markets Association

Before the

Committee on Commerce, Science & Transportation

United States Senate

"The Partnership Between NIST and the Private Sector: Improving Cybersecurity"

July 25, 2013

Chairman Rockefeller, Ranking Member Thune, and members of the Committee, thank you for scheduling today's hearing on improving cybersecurity through the NIST and private sector partnership.

My name is Mark Clancy, and I am the Corporate Information Security Officer at The Depository Trust & Clearing Corporation ("DTCC"). I also serve on the Executive Committee of the Financial Service Sector Coordinating Council and as the Vice Chairman of the Financial Services Information Sharing and Analysis Center (FS-ISAC) .

DTCC is a participant-owned and governed cooperative that serves as the critical infrastructure for the U.S. capital markets as well as financial markets globally. Through its subsidiaries and affiliates, DTCC provides clearing, settlement and information services for virtually all U.S. transactions in equities, corporate and municipal bonds, U.S. government securities and mortgage-backed securities and money market instruments, mutual funds and annuities. DTCC also provides services for a significant portion of the global over-the-counter ("OTC") derivatives market. To provide insight into the criticality of DTCC's role in the safe and efficient operation of the U.S. capital markets, in 2012, DTCC's subsidiaries processed more than $1.6 quadrillion in securities transactions.

Today, I am testifying on behalf of the American Bankers Association[1], Financial Services Roundtable[2], and the Securities Industry and Financial Markets Association[3] who collectively represent a large segment of the financial services sector.

At the highest level, we applaud and support the goals of S. 1353 The Cybersecurity Act of 2013 introduced by the leadership of this Committee. In my testimony today I will address current cyber threats, the sector-led initiatives to defend against these threats and the ways in which the Committee bill supports those efforts. Finally, I will stress the continued importance of crafting a more robust threat information sharing environment, particularly across our critical infrastructure.

CURRENT CYBER THREAT

According to McAfee and the Center for Strategic and International Studies (CSIS), there is an estimated $100 billion annual loss to the U.S. economy and as many as 508,000 U.S. jobs lost as a result of cybercrime and cyber espionage.

For the financial services industry, cyber threats are a constant reality and a potential systemic risk to the industry. Our markets and financial networks are predicated on trust and confidence. The trusted transfers and transactions that occur hundreds of millions of times a day are a

[1] The American Bankers Association (ABA) represents banks of all sizes and charters and is the voice for the nation's $14 trillion banking industry and its two million employees.
[2] The Financial Services Roundtable (FSR) represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. Roundtable member companies provide fuel for America's economic engine, accounting directly for $98.4 trillion in managed assets, $1.1 trillion in revenue, and 2.4 million jobs.
[3] The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA's mission is to support a strong financial industry, investor opportunity, capital formation, job creation and economic growth, while building trust and confidence in the financial markets. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

fundamental prerequisite for modern capital markets, investors, consumers, and governments to conduct business and drive economic growth.

Given the reliance on technology and the importance of for trust in the sector, individual institutions, and the industry as a whole perform risk assessments based on the types of attacks and threat actors they are subject to. The industry groups threat actors into four categories – Crime, Hacktivism, Espionage and War.

> ***Crime*** **-** The motivation of these groups is financial gain. The threat intensity of these groups varies based on two factors: the capabilities of the actors and the vulnerabilities of the targets. While organizations are continually assessing and addressing potential gaps in their systems, criminals are just as quickly acquiring new technical skills and capabilities through a sophisticated cyber black market
>
> ***Hacktivism*** **-** The term hacktivism is applied to groups or individuals who use computer intrusion or "hacking" techniques to promote and publicize an often radical political or cultural point of view. The most recent example of hactivism has been the distributed denial of services (DDoS) attacks for which the Cyber Fighters of Izz ad-din Al Qassam have claimed credit. These attacks against large financial institutions began in 2012 allegedly to protest the posting of the "Innocence of Muslims" video on YouTube. This group, like virtually all hacktivists, is not motivated by financial gain – it wants to make a high-profile political statement. The capabilities of hacktivists vary greatly, although it is common to find a few highly-skilled individuals operating in loose confederation with lesser-skilled, but highly-motivated actors.
>
> ***Espionage*** **-** The term cyber espionage was coined to reflect the "spy vs. spy" activity that has occurred between nations. However, cyber espionage has expanded in recent years beyond attempts to steal national secrets to now include cyber theft of proprietary information from corporations in an effort to gain an economic and competitive advantage over the commercial interests of a country.
>
> ***War*** **–** This generally refers to the launch of a cyber-missile or some other cyber weapon of mass destruction to devastate the capabilities of a government or corporation by causing a physical system to fail or to gain control over that system. Today, as many as 30 countries have cyber war units to protect and defend against such an attack, according to former Secretary of Defense Leon Panetta, who also oversaw a cyber-command center comprised of Army, Navy, and Air Force personnel. In addition, some countries are developing units to promote or instigate this type of warfare.

The universe of threat actors, regardless of the category into which they fall, pose a significant and growing danger to the sector. These threats range from theft, to disruption and destruction.

> ***Theft*** **–** Actions resulting in the theft of customer, proprietary, or confidential data or information. The loss of essential account information has the potential to put the public in harm's way for fraud and identity theft. If the crimes happen regularly, confidence in the sector could erode. The theft of a customer's access credentials when stolen via

malicious software installed on the individual's computer is particularly dangerous because that customer faces the potential loss of his or her funds and assets.

Disruption – Actions intended to cause disruptions to systems and operations, denying authorized users access to the affected systems. For example, in the previously mentioned DDoS attacks against the sector, hacktivists successfully blocked or otherwise limited the availability of certain consumer-facing websites for brief periods, but did not impact any institution's internal or critical functions. In the future, more severe cyber-attacks could attempt to target these internal, critical functions.

Destruction – Actions intended to compromise the integrity of or cause the destruction of data and systems.

Financial firms take extreme precautions to guard against these three main types of incidences that could impact the integrity of customer or institutional data. Not only is this an issue addressed by individual institutions' risk management functions, but also an issue that has interest by executive leadership to increase the investment in this critical space.

The Systemic Impact of Cyber-Attacks on DTCC

As mentioned earlier, DTCC serves as the critical infrastructure for global financial markets. As a result, the organization brings a dual perspective to its view of the cyber risk environment and its impact on critical infrastructure. First, DTCC must examine and plan for cyber-attacks that could impact its ability to perform clearance and settlement and other critical post-trade processes that underpin the global financial marketplace. Second, because of the interconnectedness of the financial system, DTCC must also take into account the broader systemic risks that could result from a cyber-attack on its systems.

The global financial system is an enormous, interconnected "system of systems." In other words, while individual institutions operate different parts of the critical infrastructure, the financial system itself is a product of the interactions of all these discrete actions. Because DTCC is connected to thousands of different market participants spanning the entire financial services industry globally, the organization must look beyond how a cyber-attack could harm its own operations to the systemic impact on its members and the broader financial community. For example, if DTCC is unable to complete clearance and settlement due to systems disruptions or outages, buyers and sellers of securities would not know if their trades had completed and, therefore, what securities they own or how much capital they have.

DTCC's financial risk and operational assessments must take into account these essential functions and determine how non-performance would impact the markets it serves as well as the firms that utilize its products and services, the investing public and the U.S. economy. In other words, if a cyber-attack directed at DTCC, or other critical financial market infrastructure, rendered its systems non-operational, what would that do to the overall functioning of the financial system? If the financial markets could not operate, how would that affect liquidity and access to capital? This systemic view of cyber risk has driven DTCC to broaden its perspective on cybersecurity to include consideration of ways to mitigate low frequency but potentially high-impact scenarios that a monoplane risk assessment would have ignored.

DTCC maintains an elaborate and sophisticated information security program to protect against the types of cyber-attacks mentioned above. This includes ongoing collaborative efforts with the private and public sectors. The financial services industry is currently engaged in a variety of public-private partnerships with the federal government to protect against cyber threats and safeguard the nation's critical market infrastructure.

SECTOR-LED INITIATVES

The financial services sector recognizes the risks, views cybersecurity as a non-competitive area and works together to identify potential threats and techniques to mitigate them. A key organization to this coordination is the Financial Services Sector Coordinating Council ("Council"), whose mission is to strengthen the resiliency of the financial services sector against cyber-attacks and other threats to the nation's critical infrastructure. The organization's leadership is comprised of industry utilities and operators, as well as industry associations, such as those on whose behalf I am testifying today.

The Council is spearheading financial services participation in the discussions surrounding implementation of Presidential Executive Order 13636 – Improving Critical Infrastructure Cybersecurity through the involvement of the ABA as co-chair of the FSSCC Policy Committee and SIFMA as lead on the incentives efforts.

The FSSCC Threat and Vulnerability Committee, co-chaired by the BITS[4] division of FSR, discuss the evolving threat to identify sector initiatives for mitigation. The Committee also developed a methodology for identifying core infrastructure for the sector along with the Department of Treasury.

The ABA, FSR and SIFMA are also collaborating with the U.S. Department of the Treasury, in concert with the Council, the Financial Services Information Sharing and Analysis Center and The Clearing House, in an effort to enhance the industry's cybersecurity ecosystem. The effort has led to the development of an Action Plan of both short- and long-term improvements to the sector's security posture focused on enhancing information sharing, increasing analysis, improving crisis management response and upgrades to core components of the cyber ecosystem.

On July 18, the industry participated in Quantum Dawn 2, a cybersecurity exercise organized by SIFMA. Five-hundred individuals from over 50 entities throughout the sector and government participated in this opportunity to run through their crisis response procedures, practice information sharing and refine protocols relating to a systemic cyber-attack. Quantum Dawn 2 was executed on a simulation platform developed as a result of cybersecurity research funding from the Department of Homeland Security's Science and Technology Directorate and was used in the exercise to simulate the U.S. equities markets. Participants are currently analyzing the findings to identify areas for improvement and best practices that will enable firms and the entire sector to better prepare for and defend against cyber threats. The exercise demonstrates the

[4] BITS, as the technology policy division of the Financial Services Roundtable, addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services.

positive linkage between research and development investments, such as simulation tools, and the ability to reduce cyber related risks through preparedness that could not have been accomplished using real world infrastructures.

Lastly, some of these initiatives involve fundamental changes to the cyber ecosystem. In December 2011, the ABA and FSR formed a new entity, fTLD Registry Services, LLC (fTLD), to apply for and run industry-related top–level domains. This decision was predicated upon an announcement by the Internet Corporation for Assigned Names and Numbers (ICANN) to allow for an unlimited number of top-level domains (TLDs) beyond the 23 existing at the time (e.g., .com, .net and .org). fTLD's goal is to represent the financial services community and to help assure that new TLDs related to the banking and insurance communities will reduce industry risk and protect customers and institutions. In addition, fTLD helps develop sound Internet practices and standards and advocates for secure Internet policies.

LEGISLATION

We appreciate and support the goals of S.1353 The Cybersecurity Act of 2013 sponsored by Senator Rockefeller and Senator Thune. If made into law, Title 1 of this bill would leverage the National Institute of Standards and Technology (NIST) to facilitate the necessary private and public sector collaboration to establish voluntary standards and best practices to better secure our nation from cyber-attacks.

As discussed in detail above, the sector believes strongly in the importance of private sector leadership for responding to this threat. We also recognize the need for a partnership between the private sector and the government. The government plays a unique role in the protection of private sector companies. To be successful the collaboration needs to include the leadership in the private and public sector as well as the practitioners who address cybersecurity related risks every day. The frameworks and standards that are rooted in the global, real world, and real time nature of the threat, are those that will achieve the objectives of the nation to reduce risk from cyber threats to critical infrastructure.

The sector works closely with our government counterpart the Financial and Banking Information Infrastructure Committee (FBIIC). The FBIIC, led by Treasury and chartered under the President's Working Group on Financial Markets, is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Essential to the sector's success is the public sector's commitment to the public/private partnership outside of the already mature regulatory regime.

The sector has participated in a number of NIST initiatives over the years and has found the organization to be ideal for the development of standards and collaboration. Most notably, the industry has been involved and continues to participate in the implementation of the National Strategy for Trusted Identities in Cyberspace (NSTIC).

Participation in the development of the Cybersecurity Framework by NIST has been a major initiative of the sector. We provided comments to NIST from the FSSCC with an emphasis on the existing national and international regulatory frameworks that the sector currently complies with. We have actively participated in the workshops and are appreciative of the specific efforts

by NIST to seek the sector's input on specific topics and understand how the Cybersecurity Framework will be used by our sector.

In addition to specifying NIST as the government organization with the responsibility to develop standards, the legislation would enable critical steps for increasing research and development for the design and testing of software, educating the workforce, preparing students for future technical jobs and promoting a National cybersecurity awareness campaign. These are all critical issues to the financial services sector.

There are two points for consideration as this bill moves forward.

In the development of a research agenda, we strongly encourage you to include the evaluation of risk management throughout the supply chain. It is important for all sectors to improve their ability to detect and defend against software and hardware components that have been tampered with during production, shipment and throughout the international supply chain process. This recommendation is based on research and discussion done by the sector in the development of the Council's research and development agenda[5].

In addition, as the NIST Director establishes a cybersecurity awareness and preparedness campaign, we encourage the Director to analyze and leverage the work already underway by the National Cyber Security Alliance. This organization, supported by a number of sectors and government partners, developed the *Stop. Think. Connect.* campaign to encourage a shared responsibility across enterprises and individuals for securing the Internet.

Need for Information Sharing Legislation

We encourage the passage of the S.1353 The Cybersecurity Act of 2013. In addition, we encourage the Senate to introduce and pass legislation that would enable increased cyber threat information sharing between the private sector and government, while providing the necessary privacy protections for individuals.

Our sector works collaboratively with our government partners to:

- Prepare for cyber-attacks by collecting, analyzing and disseminating threat information to the extent currently feasible, assessing systemic risks, and conducting joint exercises.
- Stay ahead of adversaries and reduce the number of incidents by anticipating threats, implementing countermeasures and addressing critical vulnerabilities.
- Identify incidents as they occur by implementing key controls that would improve our ability to detect and block cyber-attacks at "net speed".
- Respond to incidents in the manner that will reduce the impact and risk to the financial institution and the sector.
- Improve security posture, and minimize impact through robust forensics, investigations and learned capability.

Given the interconnected nature of cyberspace, institutions recognize that the strongest preparations and responses to cyber-attacks require collaboration beyond their own companies.

[5] http://www.fsscc.org/fsscc/news/2013/FSSCC%20RD%20Agenda%20April%2024%202013.pdf

As a result, the sector has engaged in a number of collaborative efforts. Through the FS-ISAC, participants share threat information between financial institutions and the federal government, law enforcement and other critical infrastructure sectors. The FS-ISAC also has a representative for the sector on the National Cybersecurity and Communications Integration Center floor to provide the Department of Homeland Security (DHS) insight into the financial sectors issues and incidents and provide an additional fan out for information from DHS to the sector.

Cyber-attacks are not specific to the financial services sector, but are the concern of all targeted sectors, making it essential to be able to share threat information across sectors. Currently, we all experience attacks and work within our sectors as the law allows. Viruses, trojans and other malicious software may be written to target a specific sector, but are often developed or leveraged to attack other sectors for additional purposes. Attackers are looking for methods to increase efficiency, so their ability to reuse these tools in attacks on multiple sectors accomplishes this goal. Our attackers share information related to their attacks. American businesses defending against cyber-attacks need that same capability. The ability to share information across sectors and with the government is necessary to effectively prepare, recognize and respond to attacks that hit across sectors. As our adversaries evolve, techniques become more complex, and coordinated attacks become commonplace, we need to advance our ability to respond in a collective, coordinated fashion.

The ability to share information more broadly is critical and foundational to our preparation for and response to future attacks. While we constantly review opportunities to improve the information shared within our industry, it is vital that our efforts also include sharing information across sectors and between the government and the private sector. Each company and public sector entity has a piece of the puzzle and an understanding of the threat. Our ability to share this information will greatly increase our ability to prepare and respond to threats.

Conclusion

On behalf of —the DTCC and the financial services industry, I would like to thank you for holding today's hearing to continue to raise awareness on this critical issue and for inviting us to testify. I would be happy to answer any questions.