House Committee on Financial Services
Subcommittee on Capital Markets and Government Sponsored Enterprises

Hearing on "Cyber Threats to Capital Markets and Corporate Accounts"

Mark G. Clancy
Managing Director and Corporate Information Security Officer
The Depository Trust & Clearing Corporation

June 1, 2012

Chairman Garrett and Ranking Member Waters,

Thank you for scheduling today's hearing on the important issue of cyber security and the U.S. capital markets. The Committee's strong leadership on this issue has been critical in helping to raise awareness of the serious threats posed by cyber-attacks on the financial system and fostering dialogue among the private and public sectors on effective strategies to minimize these risks.

My name is Mark Clancy, and I am the Corporate Information Security Officer at The Depository Trust & Clearing Corporation ("DTCC"). 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 2010, the Depository Trust Company ("DTC") settled more than $1.66 quadrillion in securities transactions. Furthermore, three DTCC subsidiaries last month received notifications from the Financial Stability Oversight Council ("FSOC") of proposed determinations to designate them as systemically important financial market utilities. The subsidiaries are National Securities Clearing Corporation ("NSCC"), the clearing and settlement subsidiary for equities and corporate and municipal fixed income securities, Fixed Income Clearing Corporation ("FICC"), the clearing and settlement subsidiary for U.S. Treasury, Agency and Government-Sponsored Enterprise mortgage-backed securities, and DTC, the depository subsidiary. DTCC itself, as the parent and holding company of these subsidiaries, did not receive a letter, and it does not expect one. As the primary infrastructure responsible for the clearance and settlement of nearly all securities traded in the US cash markets, these DTCC subsidiaries play critical roles in mitigating risk and ensuring the safe and seamless operation of the U.S. capital markets.

I am going to focus my testimony today on providing an overview of DTCC's approach to managing the cyber risk environment. Then I will highlight the nature of the cyber-threats DTCC faces as an organization, how DTCC and the industry plan for and respond to these potential attacks on the infrastructure and opportunities for the private sector and government to work collaboratively to enhance cooperation and information-sharing to protect the safety and soundness of the capital markets.

Understanding the Risk Environment

Due to DTCC's unique role standing at the center of the financial services industry, the organization brings a dual perspective to its view of the risk environment. 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. While these operational risks have long defined the risk landscape for DTCC, in recent years the organization has expanded its focal point to also include liquidity and market risks related to cyber-threats. 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.

To understand the nature and extent of the threats faced by DTCC, the organization regularly conducts enterprise-wide risk assessments, including a thorough analysis of business functions and the facilities, systems, applications, business processes and people that perform them. Next vulnerabilities that might exist within those assets and the controls in place to mitigate them are examined. Finally, the threats that exist to those assets are analyzed. The combinations of those factors determine the level of residual risk in the organization – that is, the risk that remains despite efforts at mitigating it.

Armed with this data, DTCC assesses whether the residual risk is above, below or consistent with the level of risk that DTCC considers acceptable (known as risk tolerance). This data informs the organization's business planning and helps guide decision-making on the need for additional investments to further reduce risk or a readjustment of risk tolerance. As these questions are considered, DTCC must also weigh the cost of achieving a tighter risk tolerance against the risk of not acting at all.

Risk assessment is a dynamic process, but certain aspects of it are more dynamic than others – and the area that is most volatile are changes in threats and vulnerabilities. On a practical level, virtually no organization has the capability to reduce threats on a daily basis. Rather, organizations must focus their efforts on mitigation of vulnerabilities and/or strengthening of controls. Vulnerabilities take many forms, and while some can be addressed relatively quickly and easily, others require complex and lengthy solutions. DTCC has numerous systems and processes in place to identify new vulnerabilities that could threaten the infrastructure, but the reality is that the organization does not control the timing of their discovery. Indeed, the only variable DTCC, or for that matter, any corporation, fundamentally controls is the tempo at which those vulnerabilities are mitigated. Through continuous analysis and review, DTCC makes decisions on investment levels in response to this rapidly-changing risk environment.

The Systemic Impact of Cyber Attacks on DTCC

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.

As mentioned earlier, DTCC serves as the critical infrastructure for global financial markets and, in this capacity, DTCC acts as an integration point that connects a wide range of industry participants. 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 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 to include consideration of ways to mitigate low frequency but potentially high-impact scenarios that a monoplane risk assessment would have ignored.

Threat Actors: Criminals, Hackivists, Espionage and War (CHEW)

It is easy to overgeneralize the threat actors who engage in cyber-crimes as identity thieves who infiltrate computer systems to steal personal data or cyber terrorists who want to declare "war" on a particular nation or the world by disrupting the efficient operation of the financial system. Richard Clarke, the counter-terrorism expert who worked as an adviser to Presidents George W. Bush and Bill Clinton, developed a simple way to classify the different "threat actors" into four distinct categories – Crime, Hacktivism, Espionage and War (CHEW). In some cases, I have modified Clarke's definitions to reflect my own views on and experiences with these subjects.

Crime

The motivation of this group is financial gain and, according to the U.S. Treasury, they have been successful. A study by the agency found that cyber-crime accounts for more revenue than international cartel drug income, running into the hundreds of billions of dollars annually. The threat intensity of this group varies based on two factors: the capabilities of the actors and the vulnerabilities of the targets. While organizations are continually assessing and addressing potential weak links 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 point of view. The most prominent example of hacktivism is the group Anonymous, which supports efforts of the website WikiLeaks to publish private, confidential information of governments and corporations to

expose what it believes are injustices or other perceived wrongs. When members of the U.S. financial sector stopped accepting payment transactions for merchant accounts from WikiLeaks, Anonymous lashed out by initiating denial of service attacks (attacks designed to make a system or network unavailable for use) against a number of those financial firms, including MasterCard, Visa and PayPal. This group, like virtually all hacktivists, is not motivated by financial gain – it wants to make a high-profile political statement. The capabilities 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. The attacks from hacktivists are more difficult to predict because their target selection is often done by consensus online and sometimes in real time.

Espionage

The term cyber espionage was coined to reflect the "spy vs. spy" activity that has occurred between nations for millennia. 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 that country.

The U.S. Office of the National Counterintelligence Executive released a report to Congress in 2011 highlighting the nature of the problem. [1]

> "In 2010, the FBI prosecuted more Chinese espionage cases than at any time in our nation's history. Although cyber intrusions linked to China have received considerable media attention, some of the most damaging transfers of U.S. technologies to foreign entities have been conducted by insiders. For example, a DuPont chemist in October 2010 pled guilty to stealing research from the company on organic light-emitting diodes, which the chemist intended to commercialize in China with financial help from the Chinese Government.
>
> Similarly, the unmasking of the network of 10 Russian "illegals" implanted on American soil indicated that these spies had been tasked to collect on economic as well as political and military issues.
>
> China and Russia are not the only perpetrators of espionage against sensitive US economic information and technology. Some US allies abuse the access they have been granted to try to clandestinely collect critical information that they can use for their own economic or political advantage." [2]

War

This is the cyber age equivalent of Carl von Clausewitz's 19th century definition that "war is the continuation of politics by other means." In this regard, war 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

[1] http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf
[2] http://www.ncix.gov/issues/economic/index.php

an attack, according to Secretary of Defense Leon Panetta, who also oversees a cyber-command center comprised of Army, Navy, and Air Force personnel.

There is another aspect of war thinking that attempts to undermine the integrity of and reduce confidence in the capabilities of a particular technology system(s) to the point that it is rendered too unreliable or error prone to be used for mission critical functions. An example would be cyber criminals tampering with the system(s) of an electronic exchange to the extent that investors lacked confidence in its ability to provide accurate prices or efficient matching of buyers and sellers.

Cyber Threats to the Capital Markets

The universe of threat actors, regardless of which category they fall into, pose a significant and growing number of dangers to the U.S. capital markets, ranging from the theft of confidential data to preventing the critical infrastructure from performing key market functions to damaging the integrity of market data and information. Let's look at each of those in more detail.

Loss of Confidentiality of Data

The loss of confidentiality of personally-identifiable information, whether the result of neglect by employees of a firm or by malicious acts of external individuals, has the potential to put the investing public in harm's way for fraud and identity theft. If the frequency of these cyber-crimes occurs are regular, it could erode investor confidence in the capital markets.

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. When this type of theft occurs on a grander scale involving thousands, tens of thousands or even millions of individual account holders, cyber criminals have the power to engage in market manipulation via "pump & dump" scams. In this example, the thieves can run up the price of a thinly-traded security they own by creating buy and sell orders in the accounts they have taken over. Their goal is to move the market in that stock by biding against themselves and anyone else they can lure into the scam.

More sophisticated criminal groups sometimes target high-value victims, including institutional clients and prime brokerage accounts, which tend to hold larger balances and normally transact with international locations, for the same purposes. The international nature of these crimes makes detection difficult.

Finally, DTCC has seen in recent years attacks using highly sophisticated social engineering techniques that target corporate deal-making information, particularly in the commodities and mergers and acquisition spaces. While this information cannot be easily converted into cash, the crimes are indicative of economic espionage and attempts to give foreign corporation or nations an advantage in competitive negotiations, such as those related to winning bids for natural resources or beating the offering price for an acquisition of a company.

Loss of Ability to Perform Market Functions

The National Market System (NMS) in the United States, which allows for the structured electronic transmission of securities transactions in real-time, is a prime target for threat actors

who want to disrupt the orderly and efficient operation of the capital markets. While there are no public reports of the NMS being directly impacted by a cyber-attack that compromised the availability of key market services in the U.S., there have been instances of such crimes overseas. For example, in August 2011 the Hong Kong Stock Exchange [3] had to suspend trading in certain securities following a denial of service attack that made corporate filing information unavailable. As a result, the securities effectively became illiquid after trading was halted, which negatively impacted both individual and institutional investors in that market.

In 2012, hacktivist groups perpetrated a series of denial of service attacks directed against the public web sites of several U.S.-based stock exchanges. These attacks, while successful in blocking the availability of these online resources for brief periods of time, did not impact the operation of the NMS, but it reinforced the determination of hacktivists to shock the public and disrupt market activity.

If an attack on the NMS were to occur, particularly one that targets critical market infrastructure(s), it could pose serious consequences for the U.S. capital markets and the broader U.S. economy. The systems in the U.S. that perform these core processing functions are largely attached to private, interconnected networks. Although the Internet is not a core component of the NMS, it is commonly used to connect market participants to various systems as a back-up to dedicated telecommunications lines or as a direct connection for smaller market participants. While this minimizes the likelihood of such an attack, mainly because it would need to be conducted from inside the infrastructure or the private networks of market participants, the issue is serious enough that it remains a primary area of concern for the financial services industry.

Loss of Integrity of Information

Maintaining the integrity of financial data is a top priority of the industry because most financial assets in today's capital markets exist overwhelmingly in digital form. The transition from a paper-based environment to an electronic one was the result of a multi-year initiative to "dematerialize" securities or "immobilize" them in centralized depositories such as DTC. Today, for example, roughly 90% of the $36.5 trillion in securities held at DTC exist only in digital form. Similarly, at the beneficial ownership level, a significant percentage of broker/dealers have digital records detailing which retail and institutional customers own which securities while custodian banks maintain that information for other institutional clients, such as pensions and mutual funds. Financial firms take extreme precautions to guard against three main types of incidences that could impact the integrity of this data.

The first incidence is loss of integrity due to accident. The digital nature of the books and records of the financial system makes it critical that this information is secure. As a result, the industry has developed an elaborate set of check and balances when changes are made to these records to protect the accuracy of data and minimize occurrences of accidental errors.

The second incidence is loss of integrity due to malicious acts. In March 2011, for example, a service provider used by both the London Stock Exchange and Italian Borsa was hosting

[3] http://www.bloomberg.com/news/2011-08-10/hong-kong-exchange-halts-some-trading-after-website-glitch-1-.html

malicious banner ads[4] on the public web sites of these exchanges. While this was not a compromise of the exchanges trading systems, it represented vulnerabilities in the supplier processes for vetting paid advertisement content. The implication of this attack is that customers who normally interact with these exchanges could have been targeted in what would have otherwise appeared to have been a normal valid business request to the web site.

Another example worth mentioning occurred in January 2011, when the European market for carbon credit trading [5]was temporarily shut down by cyber criminals who changed the ownership information of individual carbon credit owners. According to public reports, this scheme resulted in the theft of 30 million euros worth of credits from the Czech Republic, Austria, Greece, Estonia and Poland emissions market and the closure of the EU Emissions Trading System for more than a week.

The third incidence I'd like to mention is loss of integrity due to conflict between nations, terrorists and/or proxies. This type of cyber-crime involves threat actors infiltrating and maintaining access inside a system or systems of a government or corporation for the purposes of launching an attack at an undetermined point in the future. While it is somewhat difficult for a corporation to assess the likelihood of such an attack given the uncertainty in motivation of the threat actors, this has the potential to be the most catastrophic attack of the three I've mentioned today and the number of incidences has risen sharply in recent years. It is interesting to note that the more highly-skilled groups or individuals who could plan and execute such an attack tend to be more heavily invested in the orderly operation of the U.S. capital markets and, therefore unlikely to engage in this activity. However, those with less technical skills, most of whom are not as invested in the U.S. capital markets, are more likely to launch this type of attack and are working diligently to acquire the necessary capabilities.

DTCC's Approach to Protecting Against Cyber Threats

DTCC maintains an elaborate and sophisticated information security program to protect against the types of cyber-attacks mentioned above. While DTCC corporate policy calls for maintaining strict confidentiality of this information to prevent cyber criminals from knowing the full range of resources and capabilities we possess, we can share certain general information and protocols with the Committee as a way to provide insight into how DTCC safeguards its systems and the data we hold on behalf of customers and the financial services industry.

DTCC has established robust policies and procedures that provide the framework for information security within the organization. These policies cover both physical and logical security, are standards based (ISO 27001 and ISO 27002)[6] and are routinely refreshed to ensure the highest

[4] http://www.techweekeurope.co.uk/news/london-stock-exchange-site-flagged-for-serving-malware-22376

[5] http://www.praguepost.com/news/7340-carbon-credit-thieves-still-at-large.html

[6] ISO/IEC 27001and ISO/IEC 27002 is an Information Security Management System (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The full name is ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems and ISO 27002 is Information technology - Security techniques - Code of practice for information security management. The two standards together formally specifies a management approach that is intended to bring information security under explicit management control and define 'best practice' recommendations for a control foundation for the protection confidentiality, integrity, and availability of information. These are global standards that are widely used across many industries. The two standards together

degree of protection against cyber-attack. DTCC's Information Security team carries out a series of processes, including preventative controls such as firewalls and appropriate encryption technology and authentication methods as well as vulnerability scanning to identify high risks, to protect the organization and its members in the cost-effective and comprehensive manner possible.

Public and Private Sector Collaboration Helps Protect Against Cyber Threats

The financial services industry is 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. A prime example of this collaborative relationship is the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). The FSSCC was established in 2002 in response to the September 11, 2001, terrorist attacks and at the request of the U.S. Treasury Department in harmony with Presidential Decision Directive 63 (PDD63) of 1998. PDD63 required sector-specific federal departments and agencies to identify, prioritize and protect United States critical infrastructure and key resources and to establish partnerships with the private sector.

The FSSCC has 52 member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government sponsored enterprises, investment banks, merchants, retail banks and electronic payment firms. FSSCC members dedicate a significant amount of time and resources to this partnership for critical infrastructure protection and homeland security. The FSSCC does not collect dues and its success as a volunteer organization relies heavily on the time members contribute and to the expertise and leadership roles members play within their respective financial institutions and associations.[7]

The FSSCC is charged with "strengthen[ing] the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the U. S. Federal government, and coordinating crisis response – for the benefit of the Financial Services sector (the "Sector"), consumers and the U.S.A."

The FSSCC has achieved a number of successes at overseeing cyber security efforts within the sector and has played a vital role in helping to identify strategic issues and coordinate a response with federal counterparts. One particular effort was the launch of a "threat and vulnerability matrix" to gather detailed information to perform an assessment at the sector-wide level, with the goal of identifying areas of common concern. In addition, the FSSCC has served as the coordinating entity in the private sector, working with the U.S. Department of Homeland Security (DHS), U.S. Treasury and other federal agencies, in getting cleared sector personal briefed at the classified level on contextual information about cyber and physical threats.

---

formally specifies a management approach that is intended to bring information security under explicit management control and define 'best practice' recommendations for a control foundation for the protection confidentiality, integrity, and availability of information. These are global standards that are widely used across many industries.

[7] http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Carlin_0.pdf

DTCC has been actively involved with FSSCC since its inception. From May 2004 to June 2006, DTCC's current President and Chief Executive Officer, Donald F. Donahue, served under an appointment by the U.S. Secretary of the Treasury as Sector Coordinator; he later served as Chair of FSSCC from April 2005 to April 2006. Currently, DTCC officials serve on various FSSCC committees, sub-committees and working groups, including the Executive Committee, Policy Committee and Sector Wide Activities Committee.

Financial Services–Information Sharing and Analysis Center and Information Sharing
The Financial Services–Information Sharing and Analysis Center (FS-ISAC) is the primary group for information sharing between the federal government and the financial sector. It was created in 1999 in response to the 1998 PDD63, which called for the public and private sector to work together to address cyber threats to the nation's critical infrastructures. After the terrorist attacks of 9/11, and in response to Homeland Security Presidential Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to include physical threats to the financial sector.

The FS-ISAC is a 501(c)6 non-profit organization and is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services firms. Since that time, the membership has expanded to over 4,200 organizations, including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors and over 30 trade associations representing the majority of the U.S. financial services sector.

The FS-ISAC has implemented a number of programs in partnership with the Department of Homeland Security (DHS) and other government agencies to encourage and expand information sharing.

In 2011 , for example, the FS-ISAC, in partnership with DHS, became the third ISAC to participate in the National Cyber Security Communications Integration Center (NCCIC) watch floor. FS-ISAC representatives, cleared at the Top Secret/Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents and potential or known impacts to the financial services sector. This program has been extremely beneficial in providing situational awareness to the financial sector while also allowing the industry to provide feedback on threats to DHS.

DTCC was a founding member of the FS-ISAC in 1999 and continues to participate in the group's information-sharing mission. I currently serve on the Board of Directors for the FS-ISAC and as a member of the Threat Intelligence Committee (TIC). Team members are also active in the TIC, the Security Automation Working Group, Products & Services Committee, Audit and Compliance Working Group, Clearing House and Exchange Forum (CHEF) and Crisis Management team.

FSSCC & FS-ISAC: A Partnership to Combat Cyber-Threats
While the FSSCC operates at a strategy and policy level, the FS-ISAC engages with its members on operational issues. Together, the two bodies work in partnership to bring a more

comprehensive approach to cyber security. For example, the FSSCC and the FS-ISAC have been successful in partnering with DHS and the United States Treasury to obtain security clearances for over 250 individuals in the financial sector who support critical infrastructure protection.

The FS-ISAC serves as the hub of activity to coordinate information sharing on threats between financial institutions and the federal government, law enforcement and other critical infrastructure organizations. A sub-community within the FS-ISAC, CHEF was established in 2011. This sub-group played a critical role coordinating information sharing in response to a series of denial of service attacks on the public websites of U.S. stock exchanges. CHEF pooled intelligence, aggregated information about the characteristics of the attacks and shared strategies and techniques to mitigate them in near real-time. This information was shared with CHEF members and, more broadly, within the FS-ISAC and by the FS-ISAC with other ISACs, law enforcement and DHS. In addition, FS-ISAC members provided the CHEF with information about their approaches to mitigating attacks of this kind, which traditionally have not centered on the capital markets infrastructure. The key to success in managing these denial of service attacks was the level of trust that accompanied the information sharing between financial institutions themselves and these institutions and the federal government.

The FS-ISAC provides a host of additional resources for its members, including access to a library of threat information and alerts on new cyber threats and attacks. This enables the industry to more effectively monitor its own systems to determine if similar activity is occurring in their networks or to better align defenses to counter an attack before it occurs. Using the internationally recognized traffic light protocol (TLP), the FS-ISAC designates the sensitivity of unclassified information as green (can be shared with the widest audience), yellow (a somewhat narrower audience) and red (the most restricted audience) to ensure the widest but also most secure distribution of data.

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT)

There are two programs I'd like to highlight today because they are excellent examples of the enormous benefits that can be derived through a collaborative approach to information sharing between the federal government and the financial sector.

The United States Computer Emergency Readiness Team (US-CERT) leads the federal government's efforts to "improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks…while protecting the constitutional rights of Americans." [8] The US-CERT, using the traffic light protocol, provides alerts to the financial sector on observable data and indicator information, including tactics, techniques or procedures used by cyber criminals or details about the threat actors. The two most effective reports the industry receives are the Cyber Information Sharing and Collaboration Program (CISCP) alerts, which combine a range of sources and provide normalized post-analysis reporting on threat intelligence, and the Early Warning and Indicator Notice (EWIN), which provides less refined but timelier information.

[8] (http://www.us-cert.gov/about-us/)

The quality and quantity of information the financial sector receives from DHS's National Cyber Security Division (NCSD) and US-CERT has been greatly improved in the last three years and has been essential in helping to protect the nation's critical infrastructure at a time of increased threats.

The financial services sector also has the ability to leverage other federal capabilities provided by DHS and/or National Institute of Standards and Technology (NIST), including the National Vulnerability Database [9](NVD), which holds information on over 50,000 software vulnerabilities in commercial and open source software products.

Additionally, the financial sector has increasingly adopted use of the NIST Security Content Automation Protocol (SCAP) [10]suite, which includes the Common Platform Enumeration (CPE)[11] to identify types of systems and software in use and the Open Vulnerability Assertion Language (OVAL)[12] to describe the technical characteristics of a system to determine if a specific software vulnerability is present. DTCC employs SCAP to automate internal processes for the identification and eradication of known vulnerabilities within its IT infrastructure. This offers the organization a cost effective and proven way to efficiently manage vulnerabilities.

To further enhance information sharing, DTCC and FS-ISAC are collaborating with DHS and other groups to develop a protocol to automate the machine-to-machine sharing of threat reporting information to reduce inefficiencies and latency.

Opportunities to Enhance Public-Private Cyber Security Collaboration

In May 2010, FS-ISAC and federal agencies took an important step forward in partnering to counter suspected state-sponsored acts of cyber espionage by creating a pilot program, known as the Government Information Sharing Framework (GISF).[13] This pilot program allowed for the sharing of advanced threat and attack data between the federal government and about a dozen financial services firms that were deemed capable of protecting highly sensitive information. The program operated successfully from May 2010 through December 2011 and was expanded to include the sharing of classified technical and analytical data on threat identification and mitigation techniques.

Unfortunately, the program was effectively terminated by the Department of Defense (DoD) in December 2011 for reasons that were unclear to pilot participants. However, while information sharing was expected to continue through DHS, this, too, was ceased in December 2011, eliminating an important source of threat data and analysis for the financial sector. Since the termination of GISF, more than 5 organizations in the financial sector have experienced threat

[9] http://nvd.nist.gov

[10] http://scap.nist.gov

[11] http://cpe.mitre.org/index.html

[12] http://oval.mitre.org/

[13] FS-IASC executed an agreement with DHS and the Department of Defense (DoD), referred to within FS-ISAC as the Government Information Sharing Framework (GISF), based on an initiative with the Defense Industrial Base (DIB) companies, known as the Defense Collaboration and Information Sharing Environment (DCISE).

activity from actors first identified to the industry through GISF reporting. Furthermore, an assessment by FS-ISAC indicates that these threats will continue to increase in the years ahead.

There were four primary benefits and insights that DTCC and the other pilot participants gained from GISF:

1. The receipt of actionable information in a format that allowed industry participants to search for similar threat activity in their own networks.

2. The receipt of contextual information on that actionable information to better understand the risk implications of observing that threat activity.

3. The ability to adjust assessments of cyber espionage using quantifiable information on the level of malicious activity being observed, which was previously invisible to members of the financial sector. This information greatly increased the collective assessment on threats that were present from these actors and resulted in the FS-ISAC substantially escalating its level of commitment and engagement with government and other partners to identify and mitigate these potential cyber-crimes.

4. An enhanced understanding that previous threat management processes, teams and tools had insufficient capacity to consume threat data due to its raw state and the level of inefficiencies in how this information was communicated. Today, the financial sector and DHS are actively collaborating on the development of standards to support the automation of sharing and consuming threat data.

GISF was responsible for driving innovative new programs in the industry to reshape the sector's approach to assessing the multitude of risks associated with cyber espionage. This prompted many of the pilot firms, including DTCC, to revise their views on best practices for managing threat information, to expand existing information sharing activities with peers and with the FS-ISAC and to make significant additional investments in threat mitigation and detection capabilities that otherwise could not have been easily justified due the lack of understanding of the risk to the sector.

Limitations of Classified Information to Protect Against Cyber-Threats
While DHS has been able to offer security clearance to more than 250 financial sector personnel for the purposes of giving them access to classified briefings, this is not sufficient on a practicable level because the data cannot be shared broadly due to its classified nature. Furthermore, the financial industry lacks the infrastructure and processing capabilities to handle such information, which typically provides additional context on non-financially motivated threat actors and their capabilities.

Next Steps: Expanding Information Sharing Between the Public and Private Sectors
Information sharing like that which occurred under the GISF program represents the most critical line of defense in managing and mitigating cyber security risk today because it:

- Provides actionable information for the industry to protect itself from cyber criminals;

- Drives innovation and improvement in defense strategies and programs, and
- Provides a vehicle for making risk-based decisions on investments and priorities.

While GISF was successful in many aspects, its reach and impact were limited because it did not scale to the depth and breadth of the sector. As a result, it is impossible to gauge the broader benefits of the program because only 16 financial institutions served as pilot participants. However, what is abundantly clear is that information sharing today occurs at "human" speed while cyber-threats occur at warp speed. Now more than ever, an investment in standards, protocols and methods for the industry to rapidly share and consume threat and observable data is needed.

In addition, information sharing is most valuable when there is a high degree of trust among and between the financial sector and federal agencies. The more trust that exists between these institutions, the more information sharing occurs – and the better equipped each organization is to mitigate the risk of cyber-attack and safeguard its systems and data from threats.

Also, there is a need for government to invest in additional staffing, tools and repositories to strengthen the nation's defenses against cyber-attack. Based on DTCC's experience and the increased need for collaboration between industry and government in this capacity, DTCC strongly supports restarting GISF, removing its pilot status and expanding its reach within the financial sector and to other members of the Critical Infrastructure and Key Resources (CIKR) community who face these types of threats. This program, in combination with supporting enhancement for standards and normalization (with an eye toward automation), will greatly improve the efficiency of threat detection.

A potential remedy that I'd like to share regarding the lack of classified processing capability within the financial industry is to enable the critical infrastructure community to engage service providers to provide the necessary capabilities. For example, telecommunications providers could filter the critical infrastructure firm's in-bound network circuits to remove threats in real-time based upon classified threat data that could not otherwise be processed at the firm. In addition, the federal government could allow the critical infrastructure firm to build and procure needed capabilities in their own infrastructure by allowing the accreditation of classified facilities to occur for non-government contractors.

Much of the depth of the U.S. government's understanding of cyber security threats is highly classified, and the CIKR community outside of the defense arena has limited personnel with the necessary security clearances. DHS has, at present, very limited ability to "hold" clearances for CIKR personnel. For example, recently-hired veterans at DTCC who held TS/SCI clearance from their military service saw those credentials lapse when they came to the private sector.

As the sophistication and technological means of threat actors increases, the financial sector and government need to move from a static one-size-fits-all framework to a risk-based one that incorporates the dynamic nature of the cyber security threat landscape, the individual firms in the financial sector and the global nature of the capital markets. Cyber-attacks on the financial services sector represent a significant risk not just to industry participants but to the stability and integrity of the global financial system itself. There are no shortage of threat actors who, for a

variety of financial and political reasons, dedicate themselves to wreaking havoc on the systems that underpin the U.S. and global economies. While the public and private sectors have taken important steps forward in recent years to enhance collaboration, a greater degree of trust and information sharing is needed to ensure that all resources are working in concert to protect and defend the financial sector for cyber-attack. There is much progress to build on in the years ahead in these areas. DTCC stands ready to work in partnership with this Committee, the Congress and Administration and federal agencies to harden the sector's defenses against cyber-crimes.

On behalf of DTCC, I would like to thank you again for holding today's hearing to raise awareness of these issues and for allowing us to testify this morning. I would be happy to answer any questions you may have.