Testimony of Mark Graff
Vice President, NASDAQ OMX Group
Before the House Financial Services Committee
Subcommittee on Capital Markets

June 1, 2012

Thank you Chairman Garret, Ranking Member Waters and all members of the subcommittee. My name is Mark Graff. I am Vice President and Chief Information Security Officer in the Office of the Chief Information Officer at the NASDAQ OMX Group. On behalf of the NASDAQ OMX Group, I am pleased to testify on Cyber Security Issues.

Although I am new to OMX, having arrived in early April, I am no newcomer to information security, with about 25 years' experience in support of both industry and government. Most recently, I was head of cyber security at Lawrence Livermore National Laboratory, one of the crown jewels of research in this country and also a repository of many of this nation's most important secrets, such as nuclear weapon designs. I moved to NASDAQ OMX to help protect another part of America's critical infrastructure, its financial markets. I changed industries; but most of the challenges – and many of the adversaries – remain the same.

Although we are an integral part of the financial services community, NASDAQ OMX is as much of a technology company as many of the businesses that list on us. We own 24 markets, 3 clearing houses, and 5 central securities depositories, spanning six continents. Eighteen of our 24 markets trade equities. The other six trade options, derivatives, fixed income products, and commodities. Seventy exchanges in 50 countries utilize our trading technology to run their markets, and markets in 26 countries rely on our surveillance technology to protect investors and maintain a level playing field. We provide the technology behind 1 in 10 of the world's securities transactions.

NASDAQ OMX is committed to a vigorous defense of our infrastructure. NASDAQ OMX dedicates substantial capital and human resources, both internal and external, to ensure our systems are protected against a wide variety of attacks. As an expert in the methods used today to defend this nation's most highly classified networks from attack, I can tell you that we use many of the same technologies and techniques to defend NASDAQ OMX.

One key method at both institutions is the isolation of critical systems from the Internet at large. While many of the services we deliver to customers worldwide are housed on Internet-facing web servers, our trading and market systems are safely tucked away behind several layers of carefully arranged barriers, such as firewalls and network isolation zones. This is an important distinction to remember we should all keep in mind when hearing about "denial-of-service attacks" against one institution or another. Any troublemaker can run up to the front door of a

house and ring the door bell over and over. That is what most “denial-of-service attacks” amount to. Sometimes, despite our best efforts, it may be difficult to reach one of our outward-facing websites for a few minutes as a result of such vandalism. When it happens, I ask you to remember that it does not mean, to return to my homely analogy, that anyone has broken into the house.

We do not rely on isolation alone. Our comprehensive information security program uses a multi-layered approach. NASDAQ OMX is continually looking ahead, identifying potential threats to the integrity of our systems such as information compromise, unauthorized system access, physical disruption, terrorist attacks, systems failures, and denial of service attacks. We then prepare for these threats through an ongoing program of information security protection and inspection, including the implementation of physical safeguards around data centers and work spaces; a consolidated network with multiple connectivity options; a disaster recovery plan for our infrastructure; capacity management and testing; and business continuity and crisis management plans.

In developing software, we treat information security as a critical element in the life cycles of our trading and corporate systems -- from initial planning, through deployment, and as part of ongoing operation.

In all of these areas, our information security program has strong senior management and board support, integrating security activities and controls throughout our business. These controls are complemented by extensive oversight by external auditors and the Securities and Exchange Commission. NASDAQ OMX continually evaluates and enhances processes to mitigate information security risks by implementing industry best practices as promulgated by organizations like the National Institute of Standards and Technology.

Below is a summary of the processes, policies and procedures that NASDAQ OMX generally follows in connection with information security:

- Business continuity plans are robust and take into consideration real time failovers of our market trading platforms, and protects against intentional or malicious attempts to disrupt our businesses.
- Information assurance at NASDAQ OMX addresses information security designed life cycle practices and controls necessary to secure our systems.
- NASDAQ OMX ensures that information is protected against unauthorized access and use by the following:
    - Traditional firewalls augmented with application layer protection.

- Host based security controls to protect against unauthorized modification and changes to the operating systems and extensive vulnerability and patch management programs to ensure the integrity of our infrastructure.

- Application security assessments, including source code review and penetration testing (by internal as well as third-party teams).

- Robust intrusion detection controls, continually updated and augmented, as part of a 24x7 monitoring process devoted to finding and mitigating cyber threats in real time.

- Assistance from third party corporations and individuals especially experienced in dealing with advanced threats.

These controls span our entire enterprise network. Our trading systems are further protected by their unique overall resilient architecture. Each trading platform, as I previously mentioned, is logically segmented from the corporate systems. It has a single point of entry and requires two-factor authentications for access and authorization.

In addition, the system restricts the information allowed to be submitted to it through the use of a fixed set of format protocols that not only controls inputs to the trading platform, but also restricts the scope and type of information that may be retrieved from the system. Finally, the trading platform is refreshed at the end of the trading day and no data is maintained in the trading platform beyond the trading day. During the trading day, NASDAQ OMX is capable of quickly observing and reacting to changes in normal data flows. Because the architecture of the system is set up to do one thing—accept and execute trade orders—activity that is not a trade order or an execution can be immediately observed and appropriate actions taken.

For all the steps that we take, NASDAQ OMX does have serious concerns about the worldwide attacks on critical infrastructure that are being led not just by rogue hackers, or organized crime, but are being backed by national governments. It is not reasonable to expect individual companies, no matter how large or sophisticated, to independently stave off cyber attacks coordinated and backed by a foreign government. If our headquarters or our physical infrastructure were under attack from foreign missiles the U.S. Government would work with us to defend our company. The same needs to be true for cyber attacks, especially since the U.S. Government is equally under attack from these foreign entities.

It is for this reason that we at NASDAQ OMX are very pleased that both houses of Congress are looking at ways to protect our critical national infrastructure through improved sharing of information about cyber threats and vulnerabilities. NASDAQ OMX supports the House passage of H.R. 3523, "Cyber Intelligence Sharing and Protection Act". Although there are concerns about data privacy that certainly need to be addressed, the bill has several good points that are necessary to curtail the numerous cybersecurity threats faced by business and government alike. Those points include:

- The ability for companies to obtain and share cyber threat information with any other entity including the federal government;
- Such shared information cannot be used by a cybersecurity provider to gain a competitive advantage;
- Such information when shared with the federal government cannot be used for regulatory purposes;
- No civil or criminal cause of action may be taken against a company acting in good faith that chooses not to act on such cyber threats obtained or shared in connection with the bill.

NASDAQ OMX is and will continue to be a willing partner with industry peers and government at every level, cooperating to protect the integrity of our critical infrastructure. Last October, for example, during Cyber Security month, NASDAQ OMX hosted Homeland Security Secretary Janet Napolitano along with a host of law enforcement agencies and financial services companies to discuss the importance of working together to address these issues. It will be my pleasure, as NASDAQ OMX's new CISO, to continue and expand such contacts and relationships.

Thank you again for inviting me to testify. I look forward to responding to your questions.