Testimony of

Mr. Anish Bhimani

On behalf of the

Financial Services Information Sharing and Analysis Center (FS-ISAC)

before the

Committee on Homeland Security

United States House of Representatives

"DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure"

March 6, 2013

STATEMENT FOR THE RECORD

Chairman McCaul, Ranking Member Thompson, and members of the Committee, my name is Anish Bhimani, and I am the Chief Information Risk Officer of JPMorgan Chase & Co. I am appearing today as the Chair of the Financial Services Information Sharing and Analysis Center (FS-ISAC). I thank you for the opportunity to address the Committee on the important topic of roles and responsibilities of the government and private sector in the critical area of cybersecurity.

I would like to address a few points today: first, an overview of the FS-ISAC, its charter, purpose and membership; lessons learned with regard to information sharing; perspectives on the FS-ISAC membership's interaction with government agencies; and finally, recommendations around information sharing and cybersecurity governance.

FS-ISAC Background

The FS-ISAC was established in 1999 in response to Presidential Decision Directive 63. This directive, later updated by Homeland Security Presidential Directive 7, required public and private sector organizations to share information about cyber threats and vulnerabilities, with the goal of helping protect the nation's critical infrastructure. The FS-ISAC is a nonprofit organization funded entirely by its member firms and sponsors. Its membership is comprised of thousands of financial and banking institutions, large and small, and its mission is straightforward – to provide the primary industry forum for collaboration on the critical cybersecurity threats facing the financial services sector. From 12 founding members at its inception, the FS-ISAC has grown to over 4,400 organizations, including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, exchanges and clearing houses,

payments processors, and over 30 trade associations, representing the majority of the U.S. financial services sector.

The overall objective of the FS-ISAC is to provide the financial services sector with the information it needs to defend against cyber threats and risk. It acts as a trusted third party that allows members to share threat, vulnerability and incident information in a timely, trusted, and, if desired, anonymous manner. FS-ISAC information sharing services and activities include:

- Delivery of timely, relevant and actionable alerts from various sources distributed through the FS-ISAC Security Operations Center (SOC);
- Trusted mechanisms to facilitate member sharing of threat, vulnerability and incident information, in either an attributed or non-attributed manner;
- Sector-specific groups and subcommittees that provide forums for members in a given part of the sector, e.g., the Payment Processors Information Sharing Council (PPISC), Insurance Risk Council, Payments Risk Council, Community Institutions Council, and the Clearing House and Exchange Forum (CHEF);
- Bi-weekly threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities and incidents affecting the sector;
- Engagement with private security companies to identify threat information of relevance to the membership and the sector;
- Development of risk mitigation best practices, threat viewpoints and toolkits, as well as member-driven research regarding best practices at member organizations;
- Subject Matter Expert committees, including the Threat Intelligence and Business Resilience Committees, which provide in-depth analysis of risks to the sector, and provide technical, business and operational impact assessments, as well as strategies to mitigate risk; and
- Participation in sector, cross-sector and national exercises and drills, such as the Cyber Attacks Against Payment Processes (CAPP), National Level Exercise 2012, and the Cyber Storm series.

Despite the competitive nature of our industry, members of the FS-ISAC recognize that the threat from cyber attacks affects all of us, and that defending the nation's critical infrastructure is not a competitive issue. We all recognize that to effectively combat this threat, we must come together as a sector and leverage the full capabilities of our collective membership. We also know that we must trust one another. Trust, simply put, is the key to the success of the FS-ISAC, and any information sharing model.

Trust is not something that can be mandated, nor easily earned. Indeed, over the past 14 years, FS-ISAC members have worked tirelessly to engender trust amongst each other and are using all of the capabilities listed above to promote the flow of threat information across the sector. As an example, the FS-ISAC has built a model for sharing information in an authenticated, but anonymous, manner for those organizations that wish to take advantage of it. In addition, we have instituted a "traffic light" protocol, indicating levels of information sensitivity and how

information may be disseminated to the membership, partners, and other organizations. These mechanisms have effectively and efficiently enabled the amount of information shared among FS-ISAC members to grow from a mere trickle a few years ago, to a veritable (but manageable) flood today. In January 2013, members shared over 92,000 pieces of threat intelligence and approximately 400 events across the sector.

U.S. Government Interaction

Equally critical as industry collaboration is our partnership with government agencies. We could not protect ourselves against cyber attacks without extremely close collaboration, partnership, and most importantly, information sharing, with a number of government agencies – most notably, the U.S. Department of Treasury and the Department of Homeland Security, but also the Federal Reserve, Office of the Comptroller of the Currency, United States Secret Service, U.S. Cyber Command, Federal Bureau of Investigation, National Security Agency, Central Intelligence Agency, and state and local governments. Additionally, the FS-ISAC is a member of, and partner to, the Financial Services Sector Coordinating Council (FSSCC) for Homeland Security and Critical Infrastructure Protection, established under HSPD7, and works extremely closely with the Financial and Banking Information Infrastructure Committee (FBIIC), under the auspices of the President's Working Group on Financial Markets. These organizations and relationships are part of the financial sector's long history of public-private partnership with various government agencies in the area of cybersecurity.

One example of this partnership is the successful effort by the Department of Treasury, Homeland Security, FBI, U.S. Secret Service and other partners to obtain over 250 secret-level clearances and several TS/SCI clearances for key financial services sector personnel. These clearances have enabled FS-ISAC members to receive briefings on new security threats and have provided useful information to the sector to implement effective controls and defenses to combat these threats. We know that this process is not always easy, and that sponsoring private sector clearances has, historically, been difficult. But in our view, given how much cyber information is classified, it is absolutely essential that private sector representatives have access to this information. The FS-ISAC would like to see this process updated and expanded to provide more clearances to the private sector, and make it easier for this information to be shared more broadly and quickly with our members.

Another good example of partnership is the work of the National Cybersecurity & Communications Integration Center (NCCIC) at DHS. In June 2011, the FS-ISAC became the fourth private sector organization to place staff on the floor at the NCCIC. Specifically, FS-ISAC representatives, cleared at the Top Secret/SCI level, attend NCCIC daily briefs and other meetings to share information on threats, vulnerabilities, incidents, and potential impacts to the sector. These individuals interact on a daily basis with the NCCIC, routinely submit and respond to requests for information, collaborate on analyses and work with the NCCIC staff to determine what information from the NCCIC would be of use to our members, and what can be shared with whom. Over the past 18 months in particular, our presence on the NCCIC floor has greatly enhanced situational awareness and information sharing between the sector and the government, as well as across other critical infrastructure sectors that participate on the floor.

More recently, the FS-ISAC has embedded a full-time staff person on the NCCIC floor in addition to the part-time resources that were deployed last year.

One of the high points in the public-private partnership with the sector occurred in 2011 when a pilot program, known as the Government Information Sharing Framework (GISF) was launched with the Defense Department. Under the program, an initial 16 financial services firms (with a plan to expand participation later) were granted access to advanced threat information, as well as to classified analysis on threat actors and mitigation techniques. The GISF provided an invaluable service to the sector, enabling the pilot participants to receive actionable, timely, and contextual information that allowed them to search for similar threat activity in their own environments. It also allowed private sector participants to adjust their assessments of cyber espionage threats using intelligence that had previously been unavailable. The program jumpstarted new efforts across the industry and helped reshape the sector's approach to assessing cyber espionage risks.

Unfortunately, the Department of Defense terminated the pilot program in December 2011 due to funding limitations. The GISF was a significant leap forward in the public-private partnership, and represented a critical line of defense in mitigating the growing cyber threat. The loss of that information feed has already been felt, as numerous financial institutions have experienced activity from actors first identified through GISF reporting and intelligence. The FS-ISAC strongly supports not only restarting the GISF program, but also expanding its reach across the financial services sector. We urge Congress and the Department of Defense to resolve any outstanding funding or authorization issues and reinstate this crucial program.

As you can see, the financial services sector, and the FS-ISAC in particular, work in collaboration with a wide range of government agencies – probably more than anyone would imagine. At the same time, we benefit from having a strong sector-specific agency – the Treasury Department – that allows us to navigate the various government agencies involved in cybersecurity.

Specifically, the Treasury's Office of Critical Infrastructure Protection plays an invaluable role to the sector, serving as a conduit between our members and the various government agencies that play a role in critical infrastructure protection. We believe that, given its knowledge of the financial services industry, as well as its relationship with various intelligence agencies, Treasury is uniquely qualified to serve in that role. Regardless of which organization is involved, however, the key is that we receive timely, actionable data from the appropriate source, whoever that is, so that we can take the appropriate action.

Creating a useful information sharing framework

There are two critical elements to creating a useful information sharing framework: determining what information should be shared, and developing robust processes for sharing timely information.

In thinking through this problem, it is impossible to construct an effective information sharing framework without also considering what specific information we need to share to most effectively protect our infrastructure. Although much of the current debate around information

sharing has focused on the important goal of protecting personal information, we believe that much could be accomplished without ever sharing personally identifiable information.
With that in mind, here are a few examples of information we at FS-ISAC believe would be most helpful to share:

- Technical details of cyber attacks as seen on networks, in IT systems, or by victims, including IP addresses of attackers and their networks;
- Analytic content of incidents, attack patterns, and trends without revealing the organization affected;
- Analysis of technical details to determine the techniques, tools, and procedures that adversaries are using to target victim organizations;
- Contextual information about threat actor groups and campaigns;
- Information about the motivation, objectives, and capabilities of these groups or campaigns.

In addition to those most critical data elements we think must be shared, we also believe that critical infrastructure owners and operators would benefit from having a much stronger framework around *how* we share.

The cybersecurity threats the financial industry faces are coming at us faster than ever before, and are growing increasingly complex. As a result, receiving stale and outdated information is of very little value in protecting our infrastructure – in fact, it is a drain on resources, and a waste of valuable time. We are strong advocates of a framework where our respective agencies and companies can deliver relevant information very quickly, at network speed, with that information flowing in both directions.

Why is that important? Today, we in the private sector face attacks that were once directed only against major government institutions. Government agencies may have established strategies and tactics to deal with those attacks that would be valuable to those us facing similar threats. Likewise, the financial sector has collectively established strategies and tactics that may be of use to government agencies. Sharing these strategies and tools to deal with advanced threats comprehensively and quickly would do a great deal to help us all fight advanced attackers.

Conclusion

In closing, please accept my thanks on behalf of the FS-ISAC for the opportunity to address the Committee on this critical issue. The risks associated with cyber attacks and threats are real, and of paramount importance to the financial industry as a whole. The ability to share information across the sector, as well as with our partners in government and law enforcement, while still protecting privacy and civil liberties, is core to our industry and our nation's response to the growing threat.

I look forward to any questions the Committee may have.