TESTIMONY

STATEMENT OF JAMIE S. GORELICK
VICE CHAIR, FANNIE MAE

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON GOVERNMENTAL AFFAIRS
342 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, D.C. 20510

OCTOBER 4, 2001

Mr. Chairman, Mr. Ranking Member Thompson and distinguished members of the Committee, thank you for the opportunity to testify today regarding the important subject of protection of the nation's critical infrastructure.

Over five years ago, I testified before this Committee about what was then an emerging issue – the need to protect America's critical infrastructure. Since that time, the Senate Committee on Government Affairs has continued to focus on this important problem, because – as we all know – addressing it responsibly requires a sustained focus and commitment. I commend the Committee for the leadership its members have shown, and share your hope that we can keep our nation and its financial system strong through more effective infrastructure security.

In my testimony in 1996, I raised the specter of a "cyber equivalent of Pearl Harbor," and expressed my hope that we would take active measures to safeguard our country's information infrastructure before such an event. We have, in fact, done much to meet infrastructure security challenges. But in the wake of September 11th, there is a renewed need to assess where we are and where we should be.

So today, I would like to use my time to review the goals we described in 1996, and again, in 1999, in the report of the President's Commission on Critical Infrastructure Protection, and take stock of the progress made toward those objectives. Then, I'd like to offer my recommendations on where we should go from here.

For years, we have known how dependent our nation's security is on the privately held information infrastructure on which it rests. The dependencies on our information infrastructure are increasing daily, as industry – and I speak with particularity about the financial services industry – increasingly operates in a paperless environment. Typically, a large financial institution uses technology to track millions of transactions a day. And each institution is dependent on other networks for its ability to operate. The events of September 11 underscore that dependency. When those buildings were hit, in addition to other tragic consequences, the systems in them and the communications nodes under them went down. With those systems went a large part of the functionality of our financial system. The accompanying malicious code attacks – Code Red, Magistr and NIMDA – caused severe damage to both corporate and government operations.

As we consider our preparedness in light of increased uses and vulnerabilities, we need to ask ourselves two key questions:

Can we detect actual or threatened intrusions into our critical information infrastructures and warn effectively?
Do we organize and resource correctly to meet the challenges we face?

Let's first look at the issue of detection and warning. Part of our ability to do this depends on foreign and domestic intelligence-gathering on the intentions, abilities and activities of adversaries and malfeasors. We cannot discuss this question in an open session, but I would give you my assessment that much more needs to be done in this arena.

The other source of intelligence – observed threats and intrusions – are the focus of both public and private sector efforts. When President Clinton issued Presidential Decision Directive 63 (PDD-63), establishing the defense of the nation's critical infrastructures against deliberate attacks, particularly those waged in cyberspace, he presented a rather unique national security challenge, one that the federal government's national security establishment cannot solve alone. With over 90% of the U.S. critical infrastructures being privately owned and operated, assuring the delivery of services vital to the nation's defense and economy must be accomplished in public-private collaboration, with market rather than regulatory solutions being the preferred path.

Let me describe how the financial services industry interacts with the principal government agencies that have responsibility in this area.

The Commerce Department's Critical Infrastructure Protection Office (CIAO) helps proliferate vehicles for private-public cooperation. Let me describe its efforts, as they apply to financial services. Various interested industry participants have, with the support of the CIAO, formed the Partnership for Critical Infrastructure Security (PCIS). The Partnership was intended to be a collaborative effort of industry and government to assure the delivery of essential services over the nation's critical infrastructures. It began as an informal organization, chiefly supported by the CIAO, but it is now a Limited Liability Company with a board of directors, 65 member companies, and an operating budget (through dues collection) of $118,000 dollars. To date, there have been three meetings of the PCIS. More frequent interaction occurs among board members and working group chairs who meet every other week by teleconference to coordinate on-going activities. Recent examples of these activities include industry-sector work on a National Plan, coordinating a media campaign focusing on critical infrastructure protection and information-sharing between sectors and the government. The President of the Board of the Partnership is from CISCO and founding members include PriceWaterHouseCoopers, The MITRE Corporation, Fannie Mae, Bank of America and CitiGroup.

A Financial Sector Information Sharing and Analysis Center (FS/ISAC) has been formed to share information on threats, vulnerabilities and incidents in the financial services industry. The FS/ISAC was launched on October 1, 1999 and became fully operational in January 2000, supported by a trusted third party vendor (Global Integrity, a subsidiary of Predictive). It is a secure facility that provides both authenticated and, where appropriate, anonymous and confidential input. When a member chooses to submit information anonymously, no one will know who submitted the information. Member organizations can enroll by signing an FS/ISAC Membership Agreement and paying an annual fee, based on the organization' requested level of participation.

The FS/ISAC is:
A private sector partnership among eligible financial services providers
A database owned by the membership and managed a third party
An anonymous submission facility for security incidents and transmission system for alerts of serious incidents
A database structured to allow members to search for incidents, vulnerabilities, threats, and solutions, available and operated 24 hours per day, 365 days per year.

Member organizations include insured depository institutions, securities firms, investment companies, insurance companies, credit card companies, government- sponsored enterprises, clearing and settlement entities, and providers of financial technology. FS/ISAC members account for eight of the top ten commercial banks, seven of the top ten securities firms, over 80 percent of the total commercial bank assets, and over 80 percent of assets under management by the top 50 open end investment companies.

All this is good progress since the CIAO was established, but the scope and scale of our capacities are not where they need to be for us to meet the challenges we face now. The PCIS and the ISACs are volunteer-based organizations that are, for the most part, not well-known, well-funded or well-staffed. For example, while the FS/ISAC has a third-party provider who convenes members for twice yearly meetings, there is limited infrastructure for real-time communication, no emergency planning other than on a volunteer basis, and limited operational capacity to act in an emergency.

Other ISACs may be farther along. I understand that the National Energy Regulatory Council, which has become the ISAC for the electric industry, has twenty-one security coordinators in the network, available seven days a week, twenty-four hours a day (though it does not have an actual operations center). I also understand that the National Communications Center (NCC), the ISAC for the communications industry, is co-staffed by both government and industry representatives and has a truly operational capability. In addition, an Alerting & Coordinating Network (ACN) was established to link all of the NCC control centers together. All of the operation centers for various companies can communicate with each other through the ACN. Because the NCC is staffed on a full-time basis, it is able to make better progress with information-sharing. For example, it has established Concept of Operations and Participation Criteria and has made a vigorous effort to reach out to other ISACs like the FS/ISAC. An Information Sharing and Analysis System used for emergency communications was accredited this April.

In addition to the above activities, government-sponsored Computer Incident Response Teams (CIRTs) have been organized to handle computer security related incidents, such as incident detection, incident containment and incident recovery. These include the Department of Defense's Joint Task Force – Computer Network Operations Center (JIF-CNO); the Carnegie Mellon - Computer Emergency Response Team (CM-CERT); the National Security Incident Response Center (NSIRC); and the Federal Computer Incident Response Center (FCIRC). Each of these has a particular focus, e.g., on the protection of defense establishments or the provision of alerts to federal agencies, etc. Information-sharing between government organizations and industry ISACs is done on an individual basis. The PCIS has established a Task Force to develop a common taxonomy and architecture to standardize information-sharing between these government organizations and industry.

I said at the time of the President's Commission report that industry needs help in establishing the infrastructures for sharing information, developing protection standards, and issuing warnings. It has become even more clear since then that these structures do not evolve on their own and, if they do evolve, they may do so on a time-table that does not match our national security challenges. The differences among industry sector ISACs appears to correlate, in part, with the degree of governmental support or involvement, and also whether these were pre-existing industry groups that could take on this task. Each of the relevant government agencies should be responsible for affirmatively helping industry stand up and staff a structure that can bring all industry participants and relevant government participants together to meet these tasks.

Each ISAC also needs to have relationships with the others and with the various government cyber warning and analysis centers. Progress toward this goal is highly uneven and inadequate. While, for example, the information-sharing between the NIPC and the NERC is reportedly robust, the relationship with other ISACs reportedly is not as strong. The communications among ISACs is spotty at best.

The FBI's NIPC has done a good deal of work in its InfraGuard system to build trust with and to exchange information with industry. It now has 1800 member companies, including Fannie Mae. There are two impediments to its effectiveness: reservations in industry about sharing information, and resources.

Two changes in the law, previously recommended, should be considered again to increase the flow of information. The Freedom of Information Act contains many exceptions, but none protects from disclosure information that a company provides about its own vulnerability. I understand that the proposed Davis-Moran Act is one idea of how to provide some level of protection for private sector companies that voluntarily provide cyber-security information to the government.

Similarly, there evidently remain antitrust concerns limiting both the sharing of information and the development of common standards by companies working in concert. As well, there are liability concerns limiting the use of cyber-security audits and tests. The industry experts who are working on these issues can, I am sure, address the Committee's interest in these issues.

There would also, I believe, be more information flowing to the FBI about attempted intrusions if companies thought that the FBI could or would investigate the repeated "pinging" of a system, by which someone is clearly looking for entry points or vulnerabilities. To me, "pinging" is like walking around a neighborhood trying all the doors and windows. We should not consider this activity to be benign. Right now, a private company can go no further in protecting itself from a concerted effort to enter its system than to politely inquire of the Internet Service Provider from which the "pinging" emanates if it might look into the matter. The government cannot take action until the intruder has gotten through the door. It is therefore fruitless to share that information with the government.

While the government has significantly improved its ability to investigate cyber attacks, it does not appear to have adequate resources. In 1998, the FBI established a nationwide capability to investigate computer attacks, the "National Infrastructure Protection and Computer Intrusion Program," under the program management of the NIPC. The NIPC has established guidance and training curricula to build a cadre of trained investigators. The number of cases more than tripled over the last three years, to over 1200 pending investigations. In addition, the NIPC built a core of computer scientists to assist on the most complicated investigations.

But the FBI has a substantial backlog of investigations in this area, so that even if it has information about a threat or intrusion, it cannot consistently follow through to investigate. With a staff of 200 agents in this area, the FBI cannot do all the things we have asked it to: investigate actual incidents, establish InfraGuard chapters, set up data bases of 'key assets', man the detection and warning functions, etc. I would suggest that this Committee evaluate the adequacy of the resources that we apply to the protection of our national information infrastructure.

Neither the NIPC nor the Commerce Department, nor anyone in or outside of government, has the operational capacity or authority to coordinate the actions of industry in an emergency or to recover and reconstitute critical infrastructures debilitated or destroyed by an attack. The original theory was that this was primarily the responsibility of the private owners and operators of those systems. Even if that is so, someone must lead the effort. Each "lead agency" of the government charged with responsibility for each infrastructure section (Energy for electrical power; Transportation for oil and gas; Treasury for banking and finance, etc.) was supposed to develop a recovery and reconstitution plan in concert with the relevant sector. As I understand it, to date, only the NIPC and its sector, Emergency Law Enforcement Services, have developed a plan. Others have works in progress. So we do not have extant plans for recovery. We should have such plans and the capacity to limit the impact of a successful cyber intrusion, as well as the capability to work around it to keep the system running. We also need to be able to counter-attack when privately held computer systems are attacked. We have seen that terrorists understand the attractions of both governmental and private sector targets, but are we prepared to respond to an attack on these non-military targets, to fight back to prevent further damage?

Finally, as in so many issues, the many and varied responsibilities of organizations in this area could benefit from clarification to reduce redundancy and turf battles. Responsibility for the identification and the planning for protection of 'key assets' resides in the FBI's NIPC, the Commerce Department's CIAO and, as the Defense Department moves closer to a homeland security role, likely there as well. Those of us who help run key assets need to know with whom to work.

Because the framers of PDD-63 were concerned that industry would reject a government-led effort, it encouraged the proliferation of private groups to do the work that needed to be done. But now, there are the CIAO, the NIPC, the PCIS, the many ISACs, and the many CIRTs. It would be helpful to take stock, clarify and, if necessary, streamline and strengthen the structure so that it is truly robust.

That brings me to the second key question:

Do we organize and resource correctly to meet the challenges we face?

There are many, many willing partners in the private sector in this important work. For our own business continuity, we need to protect our own infrastructures and help our business partners do the same. But we are unused to collective or collaborative action like that called for here. We also have a great deal of technical expertise to share, but we are used to protecting, not sharing, our technical prowess. The ISACs and the PCIS provide for such activities, but we would be helped if we had:

coherent, cohesive leadership from the government and a clear understanding of who is doing what in the government
adequately resourced support for the establishment of robust infrastructures like the ISACs that convene industry participants, share information and plan for an emergency a legal rubric that makes it easier to share information and set common standards a robust set of

investigative resources to whom we can turn when there is evidence of an intrusion or threat of one and, in an emergency, a plan and a person or persons with authority to act on that plan.

With continued focus on the importance of these efforts, together we can better protect our critical information infrastructure.

Thank you for the opportunity to appear before you today.

Committee Members | Subcommittees | Hearings | Key Legislation | Jurisdiction
Press Statements | Current Issues | Video of Select Hearings | Sites of Interest