TESTIMONY

Final Statement of Sallie McDonald

Good morning, Mr. Chairman and Members of the Committee. On behalf of the Federal Technology Service of the General Services Administration let me thank you for this opportunity to appear before you to discuss our role in Critical Infrastructure Protection.

Background
Critical Infrastructures have long existed in the United States. The shipping systems for the transportation of goods to and from Europe represented a critical infrastructure for our first colonies. In the nineteenth century, telegraph and the railroads became critical infrastructures. As the United States developed an urban, industrialized society, utilities such as gas, electricity and water became critical infrastructures. The difference today is that all of our critical infrastructures now have a common link. Infrastructure systems that were until recently controlled by dedicated computer systems designed and created for one specific purpose are now controlled by applications that run on the same kinds of operating systems that can be found almost everywhere. The development of inexpensive, off-the-shelf computing power and the interconnectivity provided by the Internet have powered our economy, but this same interconnectivity has provided the vulnerability to intrusion and exploitation. Vital systems that control publicly and privately owned and operated critical infrastructures share common attributes that can be analyzed and exploited. The Federal Computer Incident Response Center, (FedCIRC) works to help Federal agencies protect their systems and maintain their critical operations. Other members of the Critical Infrastructure Protection community focus on helping private sector owners and operators to protect their systems and to assure the availability of critical services.

FedCIRC, is a component of GSA's Federal Technology Service. As designated by the Government Information Security Reform Act, FedCIRC is the central coordination facility for dealing with computer security related incidents within the civilian agencies of the United States Government. This Act mandates that Federal agencies report computer security incidents to FedCIRC. Our role is to assist those agencies with the containment of security incidents and to aid them with the recovery process. This directly supports the critical infrastructure protection mission because the Federal Government's agencies depend upon their computer systems not only to conduct government operations, but also to provide vital connectivity to the owners and operators of the Nation's critical infrastructures. For example, the Federal Aviation Administration's networks provide them with critical connectivity to components of the Aviation industry which enabled the FAA to rapidly execute the unprecedented grounding order in response to the acts of terror on the morning of September 11. Similarly, the Treasury Department maintains connectivity to the nation's financial services sector that is crucial to the health of the economy.

When a government agency reports a computer security incident, FedCIRC works with the agency to identify the type of incident, contain any damage to the agency's system, and provide guidance to the agency on recovering from the incident. Additionally, FedCIRC assists in identifying system vulnerabilities associated with the incident and provides recommendations to prevent recurrence. Upon receiving an incident report, FedCIRC evaluates and categorizes the incident with respect to its impact and severity. If criminal activity is indicated, FedCIRC informs the reporting agency of the requirement to immediately notify Law Enforcement, either their Inspector General or the National Infrastructure Protection Center (NIPC) according to agency policies. If the incident appears to have originated from a foreign country, FedCIRC categorizes it as potentially having national security implications and immediately contacts both the National Security Agency's National Security Incident Response Center (NSIRC)and the NIPC. As appropriate, FedCIRC advises all Federal agencies of the discovery of new vulnerabilities and exploits, and provides guidance to eliminate or reduce the vulnerability, and thwart the exploit.

Incidents involving new vulnerabilities or previously unseen exploits require in-depth analysis. Effective incident analysis is a collaborative effort. Data is collected from multiple sources, then verified, correlated and analyzed to determine the potential for proliferation and damage. This collaborative effort has resulted in the development of an incident response community that includes FedCIRC, the NIPC, the NSIRC, the Department of Defense's Joint Task Force for Computer Network Operations (JTF-CNO), the Intelligence Community's Incident Response Center (ICIRC), industry, academia, and individual incident response components within Federal agencies. Though the respective missions of these organizations vary in scope and responsibility, this virtual network enables the Federal Government to capitalize on each organization's strategic positioning within the national infrastructure and on each organization's unique access to a variety of information sources. Each entity has a different, but mutually supportive mission and focus, which enables the critical infrastructure protection community to simultaneously obtain information from, and provide assistance to the private sector, Federal agencies, the Intelligence Community, the Law Enforcement Community, the Department of Defense and academia.

The NIPC, NSIRC, JTF-CNO and FedCIRC are involved in a constant sharing of sensitive cyber-threat and incident data, correlating it with counter-terrorism and intelligence reports to develop strategic defenses, threat predictions and timely alerts. These efforts depend, not on any one participant, but on the unique and valuable contributions of each organization. The NIPC, because of its relationships with industry, is able to solicit additional participation when dealing with complex analysis issues. This broader spectrum brings together some of the nation's best talent to work on known and developing threats to the cyber infrastructure. FedCIRC's relationship with the NIPC is exemplified by the detailing of FedCIRC staff personnel to the NIPC's Watch and

Warning Unit. Alerts and advisories are frequently generated by the NIPC, NSIRC, and FedCIRC as a collaborative effort and represent a consensus when distributed to Federal agencies, industry and the general public.

FedCIRC, NSIRC and the NIPC have initiated a process to improve information sharing and analytic efforts. FedCIRC has developed a standardized reporting format to facilitate joint processing and analysis of incident information. When an incident has the potential for widespread proliferation or damage, the participating organizations routinely pool their information and skills. Cyber-incidents involving a pending or potential investigation are handled in a manner that preserves sensitive cyber-evidence without adverse impact to the affected agency's mission functions or violation of applicable privacy statutes.

The unified response to recent threats to the cyber infrastructure, including the **Code Red Worm**, and the **NIMDA WORM** clearly demonstrate how these collaborative relationships work and how each participant's contributions help to assess and mitigate potential damage. In both instances, industry alerted the incident response community to the new exploit. The Code Red Worm conducted widespread automated network scanning to identify systems operating under Microsoft's Internet Information Server software. A public advisory had been previously released identifying a serious security vulnerability that could allow an intruder to gain control of the vulnerable system and employ it to scan and infect other vulnerable systems. The first version of Code Red commanded thousands of infected computers to simultaneously flood the White House web site, which would result in a denial of service, denying access to citizens seeking information from the White House web site. The attack was thwarted in part by changing the numerical Internet address of the White House web server. This action redirected the attack against a non-existent address, negating any service impact.

During a previous event, a collaborative communication network had been established among the National Security Council, FedCIRC, NIPC, the Commerce Department's Critical Infrastructure Assurance Office (CIAO), NSA, CIA, Department of State, DoD, National Communications System's National Coordination Center (NCC), academia, industry software vendors, anti-virus engineers and security professionals. This network enabled participants to share details as they performed analysis and developed remediation processes and consensus for protection strategies. In the case of Code Red, through the collaboration of the above named groups, the collective team concluded that this worm had the potential to pose a threat to the Internet's ability to function. An unprecedented public awareness campaign ensued, concurrent with efforts to ensure that all vulnerable servers were protected. Statistical information provided by software vendors indicated an unprecedented rush by users to obtain security patches and software updates addressing the vulnerabilities. As a result, the impact of Code Red and its variants was significantly mitigated, and serious impact to Internet performance was avoided.

As this testimony is taking place, collaborative analysis and defensive strategies are being developed for a new and very serious Internet threat, the "**NIMDA Worm.**" Like the Code Red worm, NIMDA self propagates looking for vulnerable systems, but it is much smarter in its quest for victims. NIMDA does not look for a single vulnerability in Microsoft's Internet Information Server. It attempts to exploit one or more in a long list of know weaknesses and also appends hidden, hostile code to web sites so that any user simply browsing a web site may infect his/her system.

The effectiveness of our response efforts is rooted in our ability to draw on the strengths of our partners and bring to bear the best technical skills against any existing or evolving threat. Effective cyber defenses ideally prevent an incident from taking place. Any other approach is simply reactive. FedCIRC, NIPC, NSIRC, DoD, CIAO and industry components are aware that the best response is a proactive, preventative approach. In order to implement such an approach, resources must be focused on the common goal of securing the nation's critical infrastructures and the strengths of each organization must be leveraged in order to achieve the most effective results. FedCIRC, NIPC, DOD, NSIRC, CIAO and others comprise a virtual team, each offering significant skills and contributions to the common defense. These collaborative successes have evolved into a three-tiered collaboration network. FedCIRC, in support of the NSC's then National Coordinator for Security, Infrastructure Protection and Counter Terrorism, has implemented three communication groups dedicated to dealing with Technical Trends; Policy Issues; and Public Awareness Issues. This permits more effective, focused collaboration to take place concurrently, enabling individuals to participate in the groups where their talents are best suited.

Summary

Mr. Chairman, the information presented today highlights the critical and effective relationship that exists between FedCIRC and other members of the Critical Infrastructure Protection community. Though each contributes individually to critical infrastructure protection, our strength in protecting information systems government-wide lies in our collaborative and coordinated efforts. Our missions may appear to overlap in certain areas, but are actually mutually supportive, each focused on a different and critical need. I trust that you will derive from my remarks an understanding of the cyber-threat and response issues and also an appreciation for the joint commitment to infrastructure protection of FedCIRC and the other members of the critical infrastructure protection community. We appreciate your leadership, and that of the Committee, for helping us achieve our goals and allowing us to share information that we feel is crucial to the protection of our nation's technology resources.

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