Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate's
National Cyber Security Division
Testimony of Lawrence C. Hale,
Director, Federal Computer Incident Response Center
Before the
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census

Good morning, Mr. Chairman and Members of the Committee. On behalf of the Federal Computer Incident Response Center of the Department of Homeland Security let me thank you for this opportunity to appear before you to discuss "How we can protect the Nation's Computer from threats". Let me introduce myself, I am Lawrence Hale, the director of the Federal Computer Incident Response Center (FedCIRC), which is part of the DHS, Information Analysis and Infrastructure Protection Directorate. FedCIRC is the Federal Civilian Government's trusted focal point for computer security incident reporting, providing assistance with incident prevention and response.

Background

> *The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace. Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society – the federal government, state and local governments, the private sector and the American people*.
>
> "The National Strategy to Secure Cyberspace, February 2003"

The Homeland Security Act of 2002, which established the Department of Homeland Security (DHS), was one of a number of important steps taken to improve our ability to protect the Nation's Critical Infrastructures. Within DHS, Information Analysis and Infrastructure Protection Directorate is the newly established National Cyber Security Division (NCSD). The NCSD is responsible for coordinating the implementation of the National Strategy to Secure Cyberspace. Key functional areas within the Division include Risk, Threat and Vulnerability Identification and Reduction; Cyber Security Tracking, Analysis and Response Center (CSTARC); and Outreach, Awareness, and Training. The FedCIRC is an important component of the CSTARC.

The NCSD has combined the information gathering and analytical capabilities of the Cyber Watch elements of the National Infrastructure Protection Center and the Federal Computer Incident Response Center, and coordinates with the National Communications System. By doing this the NCSD not only has the added benefit of enhanced resources, but the synergy of knowledge created from the unique resources from each of the watch elements. The Federal Government's ability to limit the effects of the recent wave of worms and viruses on its networks clearly demonstrates how these collaborative relationships work and how each participant's contributions help to assess and mitigate potential damage. The NCSD has made significant progress since its inception in June 2003 by playing a central role in coordinating national efforts to deal with cyber threats and vulnerabilities. Focusing exclusively on threats (worms, viruses, etc) would force us into a reactive posture, taking action only after threat information is received, processed, and analyzed. By focusing on addressing vulnerabilities, NCSD has been successful in reducing the impact of a number of recent cyber incidents.

The NCSD is working to develop the same type of collaborative relationship with Private Sector Information Sharing Analysis Centers, State and Local Government, Law Enforcement, Academia, and Private Industry.

FedCIRC has the goal of securing the Federal Government's Cyberspace. FedCIRC, as noted in the E-Government Act of 2002, serves as the Federal Information Security Incident Center for the Federal Civilian Government. FedCIRC is the central government non-law enforcement focal point for coordination of response to attacks, promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. As such, FedCIRC must compile and analyze information about incidents that threaten information security and inform Federal agencies about current and potential information security threats and vulnerabilities.

FedCIRC demonstrated NCSD's enhanced coordination role during the recent wave of worms and viruses. (e.g. Blaster, SoBig.F). Working closely with CERT-CC and software providers, FedCIRC identified the potential impact of newly disclosed

vulnerabilities and developed corrective actions and mitigating strategies. Federal Civilian agencies were advised of the existence of these vulnerabilities, and given actionable information on reducing their exposure to the threats before attack programs were released. Patches were developed, validated and disseminated to agencies. Working closely with OMB and the Federal CIO Council, agencies were instructed to take action to address the vulnerabilities, and report their status. As a result of these measures, the Federal government was better prepared to avoid damaging impact when the exploit codes were released and the attack phase of these events occurred.

The NCSD has a number of initiatives underway to aid in threat and vulnerability reduction:

Patch Management Program: The majority of successful attacks on computing systems result from hackers exploiting the most widely-known vulnerabilities in commercial software products. The problem is not that patches to fix these vulnerabilities don't exist, but that existing patches are not quickly and correctly applied. There are several factors that contribute to this. Agencies must have a plan on how patch management is integrated into their configuration management process(es). Agencies must maintain a current inventory of assets and prioritize their assets. (e.g. mission critical, network perimeter, servers, workstations, etc). Also, with an estimated 4000 vulnerabilities being discovered each year, it is virtually impossible for most agencies to install all of the patches that are released. Therefore an organization's patching process should define a method for deciding which patches get installed first and a method for deciding which systems get patched.

FedCIRC's Patch Authentication and Dissemination Capability (PADC), a web-enabled service that provides a trusted source of validated patches and notifications on new threat and vulnerabilities is a first step. FedCIRC's vision is to build from the ability of providing validated patches to developing a more enhanced IT Configuration and Vulnerability Management program that will automate the process. By automating the process agencies will no longer have the burden of having to manually apply Patches

which will enable them more time to focus on building a more robust configuration management program which is a key part of any security strategy used to protect our critical information systems.

Data Analysis Capability: In partnership with CERT/CC, FedCIRC is piloting a study to develop real time analytical tools that may help in identifying precursors or indicators of impending attacks.

One of NCSD's goals is to have this same level of enhanced response and information sharing with the Private Sector, State and Local Government and the general Public to ensure everyone is equally prepared in our fight to prevent cyber attacks against America's Critical Infrastructures. The Federal Government has a program in place to focus on Cyber Security. State and Local Government and Private Industry must do the same to be as effective.

In addition, NCSD in its outreach and awareness function has launched its cyber security awareness initiative that includes an effort to design and lead implementation of training and awareness efforts and campaigns that use a multi-level approach to educate industry, government, and the public on the importance of their roles in National cyber security. By this effort NCSD will work with OPM and NIST to help increase the number and quality of trained cyber security professionals in the federal workforce by its efforts to facilitate and improve Cyber Corps (the scholarship-for-service program for IT security.

In closing, I would like to assure the Committee that the National Cyber Security Division is committed to building on the success that FedCIRC has achieved in helping Federal Civilian Agencies protect their information Systems from the most damaging effects of malicious code. NCSD must now translate this success to a national scale. I look forward to continuing to work with OMB and the Congress to ensure that we are successful in this important endeavor.