US Gov. Cybersecurity Experts who have left this year so far:

- **Richard Clarke** *Special Advisor to the President for Cybersecurity*
- **Howard Schmidt** *vice-chairman of the President's Critical Infrastructure Advisory Board*
- **Ron Dick** *director of the National Infrastructure Protection Center (NIPC)*
- **John Tritak**, *director of the Critical Infrastructure Assurance Office (CIAO)*

NSA's control. Wolf foresees the center involving representatives from academia, industry, the Federal government, national laboratories, and the national security community.

Wolf and other computer security experts warned of the risks posed by foreign software and software developed offshore under outsourcing contracts. Conceivably, an NSAC would examine such software for the presence of backdoors, viruses, and destructive or security-compromising bugs. Wolf said the NSAC would examine software "wherever it's written and . . . validate it [as] trusted software."

Shankar Sastry, a former Director of the Information Technology at the Defense Advanced Research Projects Agency (DARPA), defended Homeland Security's new role in cybersecurity. Challenging NSA's plan to create a NSAC, Sastry said, "DHS and HSARPA could be the place where cybersecurity research could be given marquee status." No actual proposal to establish an NSAC has yet been introduced.

Viruses & spam fuel new laws

Wayne Madsen

There is a flurry of other cybersecurity bills being introduced in Congress, some in response to the recent SoBig.F virus and Blaster worm and others resulting from the growing spam problem.

Adam Putnam of Florida, the Chairman of the House Government Reform Committee's Subcommittee on Technology and Information Policy, is considering a bill that would require companies to include a cybersecurity checklist with their regular Securities and Exchange Commission (SEC) filings. Critics of that approach contend such a requirement would not improve security but generate new business for consultancy and accounting firms.

Senators Ron Wyden and Conrad Burns are sponsoring the "CAN SPAM" bill that would require the government to prove that spammers knew they were violating the law before the government shut them down.

Another bill sponsored by Senator Charles Schumer of New York would set up a national "do not spam" registry similar to the current "do not call" registry limiting unsolicited telephone marketing calls.

However, the Chairman of the Federal Trade Commission, Tim Muris, said such laws banning SPAM could do more harm than good. He said that laws would not be enforceable since spammers frequently cross international borders.

In Brief

2 SCRIPTS KIDDIES CAUGHT FOR VARIANTS

Two script kiddies, from Romania and the US are suspected of releasing MS Blaster variants. 18-year-old American Jeffrey Lee Parson has been arrested for releasing the B variant. His variant is reported to have infected 7000 systems. A 26 year-old Romanian has been charged of unleashing MS Blaster.F on a Romanian University according to security vendor, Bitdefender.

VIRUS MEANS ACCOUNTANT ESCAPES CONVICTION

An accountant from Alabama, US has been acquitted of nine counts of tax evasion and filing false tax returns because he blamed a virus on his computer for spewing the data.

MORE RPC VULNS.

Microsoft has released another patch for three newly discovered bugs in the Remote Procedure Call (RPC) service. These vulnerabilities are different from the RPC DCOM hole exploited by MS. Blaster. Experts are predicting that a worm will soon follow.

GIANTS JOIN TO FIGHT ID THEFT

Microsoft, eBay, Amazon and Visa among others have set up the Coalition on Online Identity Theft. The plans include the release of education programmes for the general public and the promotion of technical guidelines for combatting ID theft.

AMAZON CRACKS DOWN ON SPOOFING

Amazon is suing 11 online marketers for sending emails appearing to come from Amazon.com.

ID THEFT COST $48 BILLION LAST YEAR

The US Federal Trade Comission (FTC) says that financial institutions lost $48 billion through identity theft in 2002 and 9.9 million people were victims. 67% of victims said that their credit card accounts were misused while 19% said their checkings or saving accounts were affected.

WEB HOSTING FIRM PLAGUED BY HOLES

Interland, a Web hosting company has a security breach which has caused disruptions in some of its 250 000 hosted sites. Interland has not confirmed how many hosted sites were infected with malicious code. Some reports point to Weathermaine and Trinidadexpress.com. as victims.

TWO YOUNGSTERS CHARGED FOR TROJAN

Two young British men, who were believed members of the Thr34t-Krew hacking group, have been charged with launching a Trojan horse. The Trojan is thought to exploit the Web Server Folder Traversal Vulnerability in Microsoft® IIS 4.0 and 5.0. The UK National Hi-tech Crime Unit (NHTCU) estimate that the pair caused an estimated £5.5 million worth of damage.

CREDIT CARD SCAM ARTIST JAILED

A fraudster who downloaded credit card details while working for Checkline plc, a company that processes ticket sales of customers using Heathrow Airport's train service has been jailed for nine years. Over the course of three and a half years as part of a gang Suni Mahtani, 26, reportedly stole 9,000 credit card details. The gang cloned imitation cards with the numbers and bought cigarettes in Europe to sell more cheaply in the UK for a profit. Media reports say that this is the biggest credit card fraud ever handled by UK police.