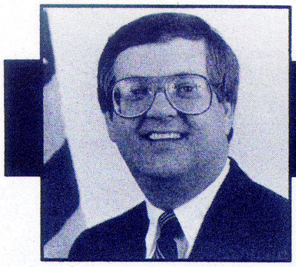

CONGRESSMAN CURT WELDON

7th District Pennsylvania

FOR IMMEDIATE RELEASE
May 17, 2001

CONTACT: Ryan Vaart
(202) 225-2539

NEWS RELEASE

STATEMENT OF HONORABLE CURT WELDON
MILITARY READINESS SUBCOMMITTEE HEARING ON INFORMATION TECHNOLOGY:
EXAMINING VULNERABILITIES OF DOD NETWORKS

The hearing will come to order.

Before we begin let me first recognize the tremendous work, effort, enthusiasm and commitment of my good friend and late Congressman, Mr. Norm Sisisky. He was committed to ensuring that the Department of Defense maintained its role as the best fighting force in the world. He will sorely be missed by not only this subcommittee, but by the Congress and the Country.

Today, the subcommittee on Military Readiness meets to receive testimony on the status of the Department of Defense information assurance programs and the measures that are being taken to establish and maintain security on the Department's information technology infrastructure.

"Hackers Cripple A State Department Computer System," "Hackers Put State, Military on Alert," "Pentagon Computers Under Assault," "Hackers Snarl White House Web site for Several Hours," these recent news articles demonstrate the vulnerability of computer networks.

Central to embracing the advantages of the Information Age is understanding the inherent risks associated with a networked military force. DoD must protect not only essential information, but also the critical infrastructures upon which information use, transport and availability depends. Today, DoD estimates its information infrastructure includes 2 to 3 million computers, 100,000 local area networks, and 100 long distance networks must be protected.

Information assurance is an essential element of operational readiness and is based on the need for accurate and timely exchange of information.

Information assurance falls under the responsibility of the Assistant Secretary of Defense (Command, Control, Communications & Intelligence). In 1998, DoD announced its plans for a Defense-wide Information Assurance Program (DIAP), with reporting authority three levels down from the ASD(C3I). A recent GAO report, "Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program," reveals the DIAP lacks a clear mission, has little authority, and does not have the support from DoD leadership. The GAO report concludes that the DIAP's limited progress leaves DoD unable to accurately determine the status of information assurance across the department, the progress of its improvement efforts, or the effectiveness of its information assurance initiatives.

Finally, the subcommittee will take advantage of the general topic of this hearing to receive an update from the Department of the Navy on the Navy Marine Corps Intranet. Last year the Department awarded a $7B contract for all information technology services. The contractor, EDS, now owns, runs, and maintains all Navy hardware and software, including Navy networks. This contract is referred to as a 'seat management' contract, as it is priced by the number of 'seats' or desktops the Navy requests. The Navy is funding the contract with money previously spend on NMCI-like costs. Much of the debate over this program was over the visibility, or lack of visibility, of the funding. There has been little debate over the benefits such a program can provide, but discussions over the funding levels remain. The Navy will provide a brief update on this program during Panel two.

###