CONGRESSMAN CURT WELDON

7th District Pennsylvania

NEWS RELEASE

FOR IMMEDIATE RELEASE
March 8, 2000

CONTACT: Maureen Cragin
Ryan Vaart
(202) 225-2539

STATEMENT OF HONORABLE CURT WELDON
CHAIRMAN, RESEARCH AND DEVELOPMENT SUBCOMMITTEE
JOINT MILITARY PROCUREMENT AND RESEARCH AND DEVELOPMENT SUBCOMMITTEE HEARING
INFORMATION SUPERIORITY AND INFORMATION ASSURANCE
MEETING THE CHALLENGES OF THE 21ST CENTURY

Today, the subcommittees on Military Readiness and Research and Development meet jointly to receive testimony on the status of the Department of Defense information superiority and information assurance programs and the measures that are being taken to establish and maintain information assurance as U.S. armed forces enter the 21st Century. We have just completed a classified briefing on the threat to the United States posed by cyber-terrorism and potential cyber-attack by Mr. Art Money, Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and Major General John Campbell, Vice Director, Defense Information Systems Agency.

Members who were present at previous Research and Development Subcommittee hearings on information technology will remember that Joint Vision 2010, the Chairman, Joint Chiefs of Staff concept for our armed forces future warfighting capability, depends upon information superiority over a future adversary as a key enabler that would provide significant advantages over adversaries during a conflict and would make both peacetime and wartime operations more efficient. However, as we have found in those hearings and as was reinforced in the June 1998 hearing on information assurance, the increasing reliance of the national defense, public and private sectors on information systems and the interlocking nature of the national defense, public, and private information infrastructures exposes us to significant vulnerabilities.

Deputy Secretary of Defense John Hamre's previous briefings to the subcommittee on the threat to DOD information systems and the measures being taken by the DOD to protect the defense information infrastructure were absolutely riveting. In June 1998, he characterized the potential for a "cyber attack" on U.S. information systems as being the "electronic equivalent of a Pearl Harbor," and said that the probability of the United States encountering such an attack was not so much "if," but "when!" In February 1999, he expanded his characterization of the threat to say that the United States and U.S. information systems were now at "war" against cyber-terrorism. This February, disruptions and denials of service by attacks on commercial network browsers and Internet e-commerce and the estimated economic loss of $1.5 billion because of those hacker attacks provide examples of the potential extension of that "war" to the private sector and highlight the need for increased emphasis on information assurance in both the domestic and national defense information infrastructures.

(MORE)

In May 1998, President Clinton in Presidential Decision Directive-63 set the goals of achieving a reliable, interconnected, and secure information system infrastructure by the year 2003 and significantly increased security for government systems by the year 2000. On January 7 of this year, the President announced the establishment of the National Plan for Information Systems Protection to strengthen our country's defenses against the emerging threat that cyber-attack and cyber-terrorism pose to our critical information systems infrastructure.

Today's hearing will provide an overview of the Administration's Critical Information Protection Program and the President's recently announced "National Plan for Information Systems Protection, discuss the Federal government's overall research and development program and objectives that support the program, and review the role of the Department of Defense in the program. These issues will be addressed by our first panel: Mr. John S. Tritak, Director, Critical Infrastructure Assurance Office; the Honorable Neal F. Lane, Assistant to the President for Science and Technology and Director, Office of Science and Technology Policy; and the Honorable Arthur L. Money, Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

They will be followed by a second panel which will focus on the role that information technology plays in the readiness of today's Armed Forces; provide an understanding of Department of Defense policy, program, and plans to achieve and maintain information superiority and information assurance among U.S. armed services; the fiscal year 2001 budget request; and supporting plans and programs of the military departments and defense agencies. The panel will also discuss specific issues of interest to the subcommittees, including the proposed Navy Marine Corps Internet. In addition to Secretary Money, members of that panel will include LTG John L. Woodward, Director, Command, Control, Communications & Computer Systems, The Joint Staff; LTG William H. Campbell, Director, Information Systems for Command, Control, Communications, and Computers, Department of the Army; RADM Richard W. Mayo, Director, Space, Information Warfare, Command and Control, Department of the Navy; LTG William J. Donahue, Director, Headquarters Communications and Information, Department of the Air Force; BG Robert M. Shea, Assistant Deputy Commandant (Command, Control, Communications, Computers, and Intelligence), Headquarters, U.S. Marine Corps.

Gentlemen, we welcome you all and look forward to your testimony.

As we begin, I would like to enter in the record a written statement submitted by the subcommittees by the General Accounting Office, which provides the agency's observations on the Department of the Navy's plan to establish a Navy Marine Corps Intranet. The Navy's proposal is of interest to both subcommittees from the standpoints of defense acquisition policy and Congressional oversight of the proposed program.

###