

**COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS
CONGRESSMAN ADAM PUTNAM, CHAIRMAN**



NEWS RELEASE

**For Immediate Release
June 15, 2004**

**Contact: Bob Dix
(202) 225-6751**

Putnam Introduces Clinger-Cohen Amendment

Washington, D.C. - Rep. Adam Putnam (R-FL), chairman of the Technology, Information Policy, Intergovernmental Relations and the Census Subcommittee, along with Rep. Tom Davis (R-VA), the Chairman of the Government Reform Committee, announced today that they have introduced a bill, H.R. 4570, to amend the 1996 Clinger-Cohen Act to place a greater emphasis on computer security within the Federal government.

This legislation updates the Clinger-Cohen Act, which requires the heads of Federal agencies to link IT investments to agency accomplishments. The Clinger-Cohen Act also requires that agency heads establish a process to select, manage, and control their IT investments. Putnam and Davis's bill would update the Act to include cybersecurity as a requirement for systems planning and acquisition by agencies and to provide the Office of Management and Budget greater authority in guiding agencies on information security issues.

"With the many threats out there today, it is vital that we factor in security when making our IT management decisions," Putnam said. "Clinger-Cohen was written before the federal government had a large web presence. It is essential that Clinger-Cohen be modernized to keep pace with these changing threats."

As chairman of the Technology subcommittee, Putnam has aggressively overseen the progress of the federal government's effort to address weaknesses in security of its computer systems, particularly the protection of information and data from the threat of cyber attacks and security breaches.

Under Davis, the full Government Reform Committee has taken the lead on procurement issues and has worked to ensure that federal government computer systems are secure.

“The on-going effort to implement e-government initiatives means that there is a high degree of interconnectivity between internal and external information systems, which exposes the Federal government’s computer networks to benign and malicious disruptions,” said Chairman Tom Davis. “Moreover, an agency’s operational efficiency relies heavily on the productive use of technology. This legislation helps ensure that every Federal information system is managed in a way that minimizes the security risks. In terms of security, it’s not how much money you spend, but how you spend it that counts.”

“Cyber attackers specifically target the federal government because of the high value of penetrating or taking over government systems. A myriad of automated attack tools are operating around the clock scanning the Internet for systems that can be taken over,” Putnam added. “I am very concerned that we may not be giving adequate consideration to security.”

“I think we all recognize that we need to bring our federal IT investment in line with the realities of the 21st century,” he continued. “I am confident that H.R. 4570 will help improve the information security profile of the federal government.”

###