

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



NEWS RELEASE

**For Immediate Release:
July 28, 2004**

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

Putnam Statement on Information Security

Washington, D.C. – Chairman Adam Putnam (R-FL) of the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census issued the following statement today on the GAO report titled, *GAO-04-376 Information Security – Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation*:

“The Office of Management and Budget’s information security policies have long required agency management officials to sign off on the technical security controls and the attendant risks associated with the operation of their information systems before the system is deployed. This authorization process is known as certification and accreditation. The enactment of the Federal Information Security Management Act (FISMA) of 2002 was an important step forward to improving information security in the Federal government and to ensuring that agencies appropriately analyze the risks associated with their systems. FISMA requires agencies to implement agency-wide risk management programs to secure their information and information systems.

“As Chairman of the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, which has oversight responsibility for the implementation of FISMA, I have been disappointed in the status of information security in the Federal government. The Subcommittee issued a report card on the 24 largest departments and agencies compliance with FISMA for fiscal year 2003. The overall grade was a ‘D’ with eight agencies receiving an ‘F.’ This followed a report card in 2002 that produced an overall grade of ‘F’ for the federal government with 14 agencies receiving failing grades. While 2003 demonstrated improvement, it is clear that greater focus and attention on reducing vulnerabilities and improving our overall information security profile is critical to the protection of federal computer networks and the information assets that they contain.

“A key performance measure of FISMA implementation under OMB’s guidance is the percentage of systems in the agency that are certified and accredited. Along with Government Reform Committee Chairman Tom Davis, I asked the Government Accountability Office (GAO) to report on the extent to which agencies’ systems are certified and accredited and to assess whether agencies’ certification and accreditation processes are consistent and effective for informing authorizing officials about the risks associated with a system. The results of GAO’s report confirms to me that it is imperative for the Congress and the OMB to continue to provide rigorous oversight to demand compliance with the provisions of FISMA, thereby improving individual agency and overall federal government information security.

“Among the 24 largest departments and agencies, GAO found that for the first half of fiscal year 2004, only 7 agencies reported that 90 percent or more of their systems were certified and accredited, 6 reported fewer than half of their systems were, including 2 departments that reported *none* of their systems were certified and accredited. GAO also found that agency processes for accounting for the number of systems that are certified and accredited were inconsistent with some agencies counting systems that were not fully certified and had only interim authority to operate.

“Given the magnitude of threats that exist today and the extent of known vulnerabilities, we must at least be able to complete an inventory of the information systems that we own and operate; perform a risk assessment; develop, implement and routinely update a risk management plan; and certify to the management, operational and technical security controls of systems that support the activities of each agency.

“I commend the departments and agencies that are being vigilant in analyzing the risk associated with their information systems before authorizing them to operate. However, I am disturbed at the overall results in this report. I eagerly await the release of OMB’s new guidance to agencies on FISMA reporting for fiscal year 2004. I hope that by the time agencies report this fall on the status of their information security that I will see greater consistency and compliance. The current information security threat environment that exists in the world today demands that the Federal government lead by example and demonstrate dramatic improvement in the information security profile of individual agencies and the overall federal government on behalf of the American people and the U. S. economy.”

The GAO report can be found at: www.gao.gov/cgi-bin/getpr?GAO-04-376

###