

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



MEDIA ADVISORY

For Immediate Release
June 23, 2003

Contact: Bob Dix
(202) 225-6751

Cyber Security Check-Up

GAO Audits of Federal Agencies Continue to Show Security Weaknesses

What: Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census Oversight Hearing: *"Cyber Security: The Status of Federal Information Security and the Effects of the Federal Information Security Management Act at Federal Agencies."*

When: Tuesday, June 24, 2003, 10:00 a.m.

Where: Room 2154, Rayburn House Office Building

Background:

The purpose of this hearing will be to explore the actions agencies are undertaking to make their systems secure, and to comply with FISMA and the results of the recently released May 2003 Government Information Security Reform Act (GISRA) report by the Office of Management and Budget (OMB)

Recent audits of 24 of the largest federal agencies continue to identify significant information security weaknesses that put critical federal operations and assets in each of these agencies at risk. The General Accounting Office (GAO), along with the Office of Management and Budget (OMB), continue to uncover many serious security weaknesses, which put critical federal operations and assets at risk.

For example, the Department of State did not report information for the FY 2001 GISRA report. It reported 3 material weaknesses for information security for FY 2002. These areas included assessing vulnerability of systems, conducting security control evaluations at least once every three years, and testing security controls. State reported, in the FY 2002 GISRA report, that none of its systems have been certified and authorized, and only 15% have an up-to-date IT security plan. Finally, State reported that only 11% of its systems have contingency plans, and of those, none had ever been tested.

In the FY 2002 GISRA report, the Department of Agriculture reported that less than 26% of its systems were in compliance with the 8 metrics that OMB reported. The agency had 70 material weaknesses in the area of information security reported by the IG. In addition, according to the IG, it is not conducting risk assessments of its systems in compliance with either OMB or GISRA requirements. The agency reports an increase in systems operating without written authority, and an increase in systems that do not have up-to-date IT security plans.

Although the Department of Treasury reported that in the FY 2002 GISRA report that 41% of its systems were assessed for risk, its IG reported that Treasury did not use an adequate methodology to determine risk. Therefore, its assessments were not valid under GISRA. There are also significant discrepancies in many of the metrics reported in the GISRA report between the Department and its IG. For example, the Department reported that 451 of its systems were reviewed. However, the IG reports that only 204 systems were reviewed. Treasury has also reported 11 material weaknesses related to information security.

While improvements are being made to secure Federal Systems the progress is slow and significant weaknesses remain. This hearing is intended to not only highlight weaknesses but to help identify solutions and ways in which the Congress can help improve the progress being made.

Witnesses:

Scott Charbo, Chief Information Officer, Department of Agriculture;
Robert W. Cobb, Inspector General, National Aeronautics and Space Administration;
Robert Dacey, General Accounting Office;
Mark Forman, Associate Director for Information Technology and E-government,
Office of Management and Budget;
Johnnie E. Frazier, Inspector General, Department of Commerce; and
Drew Ladner, Chief Information Officer, Department of Treasury;
Bruce Morrison, Acting Chief Information Officer, Department of State.

###