September 28, 2001

MEMORANDUM TO: Chairman Meserve
Commissioner Dicus
Commissioner McGaffigan
Commissioner Merrifield

FROM: Dennis K. Rathbun, Director **/RA/**
Office of Congressional Affairs

SUBJECT: HOUSE GOVERNMENT REFORM HEARING ON VULNERABILITY OF FEDERAL INFORMATION TECHNOLOGY, 9/26/01

The House Government Reform Committee's Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations held a hearing, "Information Technology--Essential Yet Vulnerable: How Prepared Are We for Attacks?" Originally, Chairman Horn (R-CA) intended to issue a report card on agencies' computer security efforts at this hearing. Earlier this month, agencies submitted to OMB their first annual reports, required by the Government Information Security Act (GISA), on their information systems security program reviews. Rep. Horn planned to base his report card on these reports; however, OMB declined to share the reports with GAO or the Hill. Instead, OMB will release a composite report early next year as part of the FY03 budget submission. Rep. Horn might issue a report card then.

Rep. Horn opened the hearing by decrying the federal government's slow progress in addressing computer security concerns, noting that information security has been on GAO's high-risk list since 1997. GAO testified that there are serious and widespread federal computer challenges that could have a broad impact, but that GISA should provide the catalyst to accelerate agencies' efforts. While agencies have moved forward with business continuity planning, many of these plans have not been fully tested. GAO's areas of focus are security program management, access controls, software development and change controls, segregation of duties, operating systems controls, and service continuity. GAO noted that as agencies focus on these areas, more weaknesses have been identified, but this likely is not that the problem is becoming worse, they are just being highlighted due to GISA.

The need for adequate resources for agencies' implementation of Presidential Decision Directive 63, a strategy for federal infrastructure protection against computer-based attacks, was emphasized by many witnesses, as was the need for the federal government to fund the long-term research needed to advance computer security. Rep. Horn asked whether the new Office of Homeland Security should be in charge of computer security: the Information Technology Association witness advocated for such a role, while GAO emphasized that at the

CONTACT: Laura Gerke, 415-1692

least, coordination of federal computer security strategies needed to occur. GAO and Rep. Horn also urged that the momentum from information security efforts initiated during Y2K preparations should not be lost.

Separately, Senator Bennett (R-UT) recently introduced S. 1456, the Critical Infrastructure Information Security Act. This bill would promote sharing of critical infrastructure information between and among the private sector and federal government and encourage them both to conduct better analyses of such information.

The witness list is attached; testimony is available in OCA.

Attachment: As stated

cc: SECY
OGC
OGC/Cyr
EDO
NRR
NMSS
RES
OIP
OCAA
OPA
OIG
CFO