November 14, 2001

MEMORANDUM TO: Chairman Meserve
Commissioner Dicus
Commissioner Diaz
Commissioner McGaffigan
Commissioner Merrifield

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

SUBJECT: HOUSE GOVERNMENT REFORM HEARING ON COMPUTER SECURITY, 11/9/01

The House Government Reform Committee's Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations held an oversight hearing, "Computer Security in the Federal Government: How do the Agencies Rate?" At the hearing, Chairman Horn (R-CA) issued a report card (see my memo of November 9 which provided the report card) on federal agencies' computer security efforts. The NRC received an "F," as did 16 out of the 24 agencies evaluated as well as the federal government as a whole.

Chairman Horn stated that while current post-September 11 efforts are focused on rebuilding infrastructure, the risk of cyberattacks cannot be ignored. He was disappointed in agencies' grades, and hopeful that the grades and the Government Information Security Reform Act ("Security Act"), enacted last year, would encourage the Administration to "work expeditiously" to address vulnerabilities. He specifically mentioned the NRC's "F" in his opening statement, noting that the agency oversees nuclear facilities and other programs (his written statement erroneously stated that the NRC oversees the nation's nuclear weapons).

GAO's Mr. Dacey testified that there were pervasive weaknesses which placed federal computer systems at risk -- that is why information security has been on GAO's high risk list since 1997. Mr. Dacey said that the volume and sophistication of cyberattacks are increasing, with a limited ability to detect them, in an environment of increasingly complex interactivity. He commended recent initiatives such as the CIO Council's guidance for information security programs and the creation of the Office of Homeland Security with responsibility to coordinate cybersecurity efforts, but he urged that agencies improve self-monitoring, that Congress use those monitoring results for oversight, and that expanded research for information security protection occur.

OMB's Associate Director for Information Technology and Electronic Government, Mark Forman, emphasized that security planning should be tied to agencies' capital planning and budget processes, emphasizing that just adding money, without a focus on the details, would not solve IT security. OMB is beginning to review agencies' first annual Security Act reports

CONTACT: Laura Gerke, 415-1692

(submitted in September), but it is too early for individual assessments. These reports included IGs' annual independent evaluations of the security program and an agency's executive summary of issues. Problems Mr. Forman noted so far were failures to: follow the implementing guidance of the Security Act, integrate security into capital plans, recognize the risk of interconnectivity, and improve employee training. Chairman Horn asked how OMB would use the Security Act data; Mr. Forman replied it would be utilized in communications for the FY 2003 budget process. Asked when OMB would submit its comprehensive Security Act report to Congress, Mr. Forman did not have a specific date, but expects the report to be submitted with or close to the budget submission next year, in order to parallel the budget's enforcement mechanism. As the budget process proceeds, Rep. Horn requested information on agencies' IT requests that are not funded because they were not documented.

Rep. Horn asked if CIOs and career employees take the security challenge seriously; Mr. Forman assured him that they do, while noting that 80% of the federal IT workforce is contractors. Rep. Horn asked how the upcoming retirements would be addressed; Mr. Foreman referenced a training program to ensure the correct skill sets, including a core curriculum developed by the CIO Council for IT workers. Rep. Horn also inquired what would have happened if a cyberattack had accompanied the physical attack on September 11th. GAO responded by noting that the nim da. worm virus over the summer, while not as press worthy, had helped to focus agencies' attention on the challenge. When asked whether there had been any computer security improvement, GAO noted that advances are unevenly occurring at agencies, but the pace of risks is high and computer security, unlike Y2K, is not a static target.

The witness list and Rep. Horn's statement are attached; testimony is available in OCA.

Attachments: As stated

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