April 9, 2001

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

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

SUBJECT: HOUSE ENERGY AND COMMERCE HEARING ON FEDERAL COMPUTER SECURITY, 4/5/01

The House Energy and Commerce Committee's Subcommittee on Oversight and Investigations held the first in a series of hearings on the security of government computer systems; dates of other hearings have yet to be announced. The purpose of this hearing was to provide an overview of the challenges facing the federal government's computer systems. The Chairman of the full Committee, Rep. Tauzin (R-LA), participated in the hearing and indicated his strong support for oversight of this issue.

There is widespread congressional interest in cybersecurity. Late last year, Congress approved the Government Information Security Act. The Act strengthens OMB's role in coordinating security of federal information systems, requires the development of government-wide standards for information security controls, requires annual evaluations of agencies' information security programs and practices, and enhances training in information security. Additionally, the House Government Reform Committee's Subcommittee on Government Management, Information, and Technology held five hearings last year on computer security. Last September, the Chairman of that Subcommittee, Rep. Horn (R-CA), issued a report card on computer security; the grades were based on agency responses to a Subcommittee questionnaire as well as audits by the GAO and Inspectors General. The NRC, DOE, FEMA, and DOT were the only agencies to get "incompletes," because there "has been insufficient auditor scrutiny to validate their self-evaluations." Overall, the federal government received a D-.

On March 16, 2001, the NRC responded to a letter from Subcommittee Chairman Greenwood (R-PA) regarding implementation of the Government Information Security Act. Although he is still awaiting documents from some of the fifteen agencies to whom he wrote, Rep. Greenwood said that he is "not pleased" with the responses. He noted that many agencies' infrastructure assessments were incomplete and that few agencies do automatic vulnerability scans, even though those scans frequently indicate shortcomings. He commented that "few, if any" do penetration tests, and most of those were limited tests as part of financial audits. Rep. Greenwood commended those agencies that test, but he stressed that more testing was needed. He criticized agencies for not taking corrective actions, noting that the number and

CONTACT: Laura Gerke, 415-1692

sophistication of cyber-attacks were increasing, yet many of those attacks occurred where problems were known and fixes available.

Rep. Davis (R-VA), was a guest member of the Committee in order to advocate both for the creation of a federal CIO as a separate entity within the Executive Office of the President and to encourage information sharing among agencies to focus greater attention on and facilitate solutions to cyber threats. The FBI witness described that agency's increasing caseload of federal computer intrusions, and the GSA described its Federal Computer Incident Response Center (FedCIRC) which coordinates activity associated with security related incidents affecting federal computer systems; such incidents must be reported to FedCIRC.

GAO testified that since 1997, information security has been on its list of high-risk issues facing the federal government. The many efforts of agencies to address security were noted, but GAO stressed the need to "maintain the momentum." GAO suggested that 1) federal information security roles and responsibilities be delineated, 2) more specific guidance on computer security controls be provided to agencies, 3) routine periodic audits be conducted, 4) the audits be used for oversight purposes by Congress and the Executive Branch, 5) adequate technical expertise by maintained, and 6) sufficient resources for computer security be provided.

Chairman Greenwood asked GAO what collective grade the federal government should receive for information security practices. While noting that problems were pervasive, GAO deferred to Rep. Horn for grades; GAO added that grades would not have changed much since the report card last year. Both Rep. Greenwood and GAO held out hope that implementation of the Government Information Security Act would cause improvement. He questioned whether some agencies' efforts were just "paperwork exercises;" GAO replied that information security should be considered a management responsibility, rather than just an audit function.

OCA will continue to monitor congressional activity on computer security. The witness list is attached; testimonies are available in OCA.

Attachment: As stated

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

Protecting America's Critical Infrastructures: How Secure Are Government Computer Systems?
Subcommittee on Oversight and Investigations
House Energy and Commerce Committee
April 5, 2001

Witness List and Prepared Testimony

Panel Demonstration
Mr. Glenn Podonsky
Office of Independent Oversight and Performance Assurance:
US Department of Energy
1000 Independence Avenue, SW
Washington, DC, 20585

Panel 1
Mr. Tom Noonan
President
Internet Security Systems
6303 Barfield Road
Atlanta, GA, 30328

Ms. Sallie McDonald
Assistant Commissioner
Office of Information Assurance
and Critical Infrastructure: US
General Services Administration
7th & D Street, SW Room 5060
Washington, DC, 20407

Mr. Ron Dick, Director
National Infrastrucure Protection
Center: Federal Bureau of
Investigation
935 Pennsylvania Avenue, NW
Washington, DC, 20535

Panel 2
Mr. Robert Dacey
Information Security Issues
U.S. General Accounting Office
441 G Street NW Room 5T37
Washington, DC, 20548

Mr. John Tritak, Director
Critical Infrastructure Assurance Office: US Department of Commerce
1401 Constitution Avenue Room 6095
Washington, DC, 20230