

October 4, 2001

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

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

SUBJECT: SENATE GOVERNMENTAL AFFAIRS HEARING,
"CRITICAL INFRASTRUCTURE PROTECTION: WHO'S
IN CHARGE?" 10/04/01

The Senate Governmental Affairs Committee held this hearing to examine the nation's readiness to deal with terrorism attacks on computer infrastructure. Senator Bennett (R-UT) noted that with Y2K preparations the country demonstrated that it could address computer failures caused by accident; now it needed to demonstrate the ability to address failures caused on purpose.

Senator Cleland (D-GA) commended the Clinton Administration for taking the initiative with Presidential Decision Directive 63 (PDD 63), which established a strategy for protecting critical infrastructure from computer-based attacks. Senator Thompson (R-TN) criticized PDD 63's implementation, noting that GAO issued a report last week stating its uneven progress, particularly because there was not a national plan identifying the roles and responsibilities of federal and nonfederal entities. These two Senators, as well as Senators Carnahan (D-MO) and Collins (R-ME), anticipate that the Executive Order which will be issued to establish the Office of Homeland Security will provide clarity and establish responsibility for computer security within that Office.

Senator Bennett has introduced S. 1456 to encourage information sharing between the private sector and government about computer attacks. The bill provides exemptions from antitrust requirements, so companies could work together, and exemptions from the Freedom of Information Act, so that computer security threats could be reported confidentially, would be provided. Senator Voinovich (R-OH) commented that the overriding concern was the human capital crisis facing the Federal Government: with many employees eligible to retire, do agencies have the people and qualifications needed to get the job done?

PDD 63 assigned overall responsibility for policy development and coordination for critical infrastructure assurance to the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council. Additionally, PDD-63 established the Critical Infrastructure Assurance Office as an interagency office located at the Department of Commerce to support the National Coordinator's policy functions. The Federal Computer

CONTACT: Laura Gerke, 415-1692

Incident Response Center at GSA is the central coordinating facility for computer security incidents in civilian agencies and assists with recovery efforts. The FBI's National Infrastructure Protection Center (NIPC) is responsible for gathering information on threats to infrastructure and for "facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts."

Senator Cleland asked the three witnesses, "Who is in charge?" They replied that the National Security Council is currently in charge, but that is subject to significant change whenever the forthcoming Executive Order is issued. The Senator commented that answering his question was also difficult for Congress to do, since Congressional committees had overlapping jurisdictions. Senator Bennett noted that other agencies do not recognize NIPC's importance and are not assisting with its analyses. The NIPC witness agreed that there had been problems in the past with interagency cooperation and provision of resources, but that situation had improved. Additionally, the Executive Order would identify a lead for analysis. Senator Carnahan asked whether additional resources were needed, the FBI replied, "absolutely." Senator Domenici (R-NM) noted that his bill, S. 1407, the Critical Infrastructures Protection Act, would provide the National Infrastructure Simulation and Analysis Center (NISAC) based at Los Alamos and Sandia, with funding to facilitate understanding of the interdependencies of the nation's infrastructures.

Congressional interest in computer security remains high; see my memo to you of September 28, "House Government Reform Hearing on Vulnerability of Federal Information Technology." Additionally, the House Science Committee may hold a hearing next week addressing computer security research needs.

Testimony is available at: http://www.senate.gov/~gov_affairs/100401witness.htm; the witness list is attached.

Attachment: As stated

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