THE CONGRESSIONAL REPORT

Reporting for the week ending June 28, 1996

- **SENATE PASSES NBC AMENDMENT**
- **SENATE EXAMINES COMPUTER SECURITY**

SENATE PASSES NBC AMENDMENT

During the past week the Senate continued to consider its version of the national defense authorization (S.1745.) Several key floor amendments were debated and passed including the Nunn/Lugar/Domenici amendment authorizing funds to establish measures to protect the security of the United States from proliferation and use of weapons of mass destruction. This amendment, which passed by a 96-0 vote on June 26, authorizes funding and provides policy guidance in the following categories:

- Emergency response assistance program: The DoD is designated to carry out a program to provide civilian personnel of federal, state, and local agencies with training and advice regarding emergency responses due to a nuclear, biological, and chemical (NBC) threats. $35M is authorized for such purposes.
- NBC emergency response: While the DoD is designated the coordinating agency in responding to the identification and dismantlement of any chemical and biological weapon and related technologies, the DOE maintains responsibilities for nuclear devices and related materials. $15M is provided for (NEST) programs while a separate $15M is provided to the DoD chemical, biological program.

- Testing of preparedness for DOE emergencies involving NBC weapons: The DoD is designated as the agency to develop and execute programs for testing and improving responses for local agencies to NBC emergencies. $15M is authorized for such purposes.
- Interception of NBC weapons and related materials at U.S. borders: $15M is provided for the procurement of detection equipment.
- International border security: The DoD is designated in cooperation with Customs, in assisting customs officials and border guards in the independent states of the FSU, the Baltic States, and East European countries in preventing the unauthorized transfer of NBC weapons and related materials. $15M is provided for such purposes.
- Nonproliferation and counterproliferation research and development: $19M is provided to the DOE and $10M to the DoD for research and development of technical programs for detecting the presence, transportation, production, and use of NBC weapons and related materials.
- Control and disposition of NBC weapons and related materials: $15M is authorized for materials control for the DOE, and $10M is made available for the Cooperative Threat Reduction Program for the DoD.
- Verification of dismantlement and conversion of weapons and materials: $10M is provided for continuing and expanding cooperative activities with the Russian government to develop and deploy technologies for improving verification of nuclear warhead dismantlement as well as technologies for converting plutonium from weapons into forms better suited for long-term storage, non weapons use, and the facilitation of verification. This provision implicitly provides funding for LANL's ARIES program.

- Elimination of plutonium production: The DoD in consultation with the DOE, is to develop a core conversion program for Tomsk-7 and Krasnoyarsk-26 leading to reactor cores that are less suitable for the production of weapons-grade plutonium. $16M is authorized for such purposes.
- Industrial partnership programs to demilitarize NBC facilities: The DOE is mandated to expand the IPP program to include coverage of all of the independent states of the FSU. No additional funding is authorized for IPP. $15M is provided to the DoD Defense Enterprise Fund to support the conversion of biological and chemical facilities.
- Lab-to-Lab program: $20M is authorized for the DOE Lab-to-Lab effort.
- Cooperative activities on security of highly enriched uranium used for propulsion of Russian ships: The DOE is designated as the agency responsible for carrying out U.S. cooperative activities with the Government of the Russian Federation on improving the security of highly enriched uranium that is used for propulsion of Russian military and civilian ships. $6M is authorized for such activities.
- Military-to-Military relations: $2M is authorized for expanding military-to-military programs between the U.S. and FSU security forces that focus on countering NBC threats.
- National coordinator on nonproliferation: The President is responsible to designate an individual to serve in the Executive Office of the President as the National Coordinator for Nonproliferation Matters. Moreover, a National Security Council Committee on Nonproliferation is established.
- Comprehensive preparedness program: The President, acting through the Committee on Non-proliferation, is responsible for the

development of a comprehensive program for carrying out the provisions of this amendment and shall report to Congress, in the FY98 budget submission, a program development plan.

In other Senate floor action, an amendment was offered by Sen. Kyl (R-AZ) to authorize underground nuclear testing until a Comprehensive Test Ban (CTB) was approved and entered into force. This amendment was rejected by a 55-45 vote. Additionally, an amendment by Sen. Nunn (D-GA) on behalf of Sen. Feinstein (D-CA) was offered to fund basic research in seismic monitoring. More specifically, the amendment authorizes $6.5M for basic research in nuclear testing monitoring to ensure that the DoD is able to support a CTB. The defense authorization was pending a vote of final passage as this report was being prepared.

SENATE EXAMINES COMPUTER SECURITY

In June 25 testimony before the Senate Permanent Subcommittee on Investigations, CIA director John M. Deutch warned that the country is likely to experience some "very large and uncomfortable" disruptions of vital computer systems at the hands of foreign terrorists or hostile nations in coming years, but pledged a major new U.S. effort to detect and combat the threat of computer break-ins.

According to Deutch: "We have evidence that a number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks" on military-related computers. Deutch added that he is convinced that foreigners are becoming increasingly aware "that advanced societies, especially the United States, are increasingly dependent on open and potentially vulnerable" computers to control electric power, airplane traffic,

telecommunications and financial operations -- posing an attractive target for virtually "any nation or foreign terrorist organization."

Deutch said "we are not well-organized as a government to address these issues" and cautioned that making vital computers much less vulnerable to attack may take decades. Deutch said that he had drawn up plans to create an office at the National Security Agency to be called the Information Warfare Technology Center, which will focus on analyzing the risks that foreign hackers pose to U.S. computers and help create new methods of investigating and defending the U.S. against electronic break-ins. Deutch also said that he supports creating a "real-time response center" for any major domestic or foreign attacks against civilian computers under the supervision of the Justice Department, as well as a separate, Defense Department center for responding to attacks on military-related computers.

Deutch disclosed that the intelligence community conducted an extensive survey last year of the risks of an attack on computers controlling U.S. telephones, the electric power grid, oil refineries and other utilities. He said the results are classified, but added that a new, broader estimate of the threat is to be completed by December. He also said the intelligence community has begun to hunt more diligently for evidence of any foreign intent to attack U.S. computers, any sign of foreign sponsorship for U.S.-based computer hacking activities, and for any indication that foreign organized crime figures are becoming involved in attacks on computers at U.S. financial institutions. The Defense Intelligence Agency, moreover, is trying to develop a way to predict a major "information warfare attack" against the United States, Deutch said.

Senator Sam Nunn noted that one obstacle is that banks and other private institutions have been reluctant to divulge any evidence of computer

intrusions for fear that it will leak and erode the confidence of their customers. Deutch responded that "the situation is improving" but that more cooperation was needed from major corporations. He said the CIA remains willing to share information with such firms about the risks they might face.

Although he declined to cite any specific examples of computer warfare, Deutch said he would list it as the second most worrisome threat to U.S. national security -- just below the threat posed by foreign chemical, nuclear, and biological arms.

Compiled by Pat Anderson, Bill Fite, and Patrick Garrity, Government Relations.