GOVERNMENTAL AFFAIRS COMMITTEE
MARK-UP OF COMPUTER SECURITY BILL
OPENING STATEMENT
March 23, 2000

Thank you, Mr. Chairman, for hastening along the mark-up of this bill, which I think will lay the security groundwork for much of the digitalized work government performs over the next several years. As we charge headlong into the future of electronic services, we understand there may be inherent trade-offs for the efficiency and cost-savings government will surely reap. I must emphasize in the strongest possible terms, however, that information security cannot be one of them. Maintaining the integrity, the availability and the confidentiality of information stored on federal computer databases is "mission critical" to serving taxpayers in the Internet age.

The cornerstone of **S. 1993, the Government Information Security Act**, is the plan each agency must develop to ensure the protection of sensitive federal information systems. Agency heads - or chief information officers - would be responsible for developing and implementing the security program, which will have to pass muster by OMB and undergo annual audits.

Because we need to change our cultural attitudes toward information security, the OMB also would be responsible for establishing government-wide policies promoting security as a central part of each agency's operation. And we intend to hold agency heads accountable, for information security is an area in which we cannot afford to fail.

We have had, and will continue to have, a lot of help in constructing this bill. One of the best ideas I have seen is the **Federal Cyber Service**, contained within President Clinton's critical infrastructure protection plan, announced in late January. Our bill authorizes this program and gives the agencies the flexibility they need to implement different components of it. Among these are scholarships in exchange for government service, retraining computer information specialists, and, as part of our campaign to influence cultural behavior, promoting awareness of cyber-security among high schools, secondary schools and among federal workers.

We did have a few issues to smooth over with the administration, particularly on the issue of whether to include national security systems under the same management structure as other government systems. But I hope we have reached an accommodation that will give defense and intelligence agencies the control they seek while holding them accountable, as we're insisting upon.

The substitute amendment the chairman and I will be offering today would require DOD and the intelligence agencies to adhere to the same management structure every other federal system must adhere to under our bill. This means they must develop a plan addressing security upgrades, although the plan need not be approved by OMB. They will also have to submit to annual audits, but they may designate their own auditors, in the interest of protecting sensitive information and system vulnerabilities. In addition, DOD and the intelligence agencies may develop their own procedures for detecting, reporting and responding to security incidents.

Mr. Chairman, I think these are the primary points I wanted to emphasize. This bill is essential to the future operations of government, and, again, I am pleased we're moving ahead quickly because in the digital age, one simply can't move quickly enough. Thank you.