

MAY 1, 2002

**SCHAKOWSKY STATEMENT DURING GOVERNMENT REFORM SUBCOMMITTEE  
HEARING ON COMPUTER SECURITY**

WASHINGTON, D.C. - This is the Subcommittee's fourth hearing on computer security in this Congress, and the message has been uniformly dismal. Agencies are not doing the basic tasks necessary to protect government computer systems. Most of our witnesses have told us the same story. Computer security is not rocket science; it is performing some basic functions repeatedly and consistently. We have all heard witnesses testify about basic functions like changing the password when installing new software, and programs that force users to routinely change their password, go a long way towards improving security.

Unfortunately, management has not made security a priority, and as a result, it has not been a priority for the staff. The Government Information Security Reform bill was an attempt to make security a priority for management. It was a step in the right direction, and the bill before us today is a substantial improvement.

H.R. 3844 requires the same agency security reports and Inspector General reports that the Subcommittee used in grading the agencies last fall. Now we must assure that Congress has access to those reports. H.R. 3844 improves upon past legislation by bringing the National Institute of Standards and Technology into the process. This bill requires an agency to assess the risk associated with its systems, and requires NIST to provide the agencies with guidance on the best way to secure against those risks.

There does seem to be one significant hole in this legislation. As we learned in confronting the Y2K problem, we can't be sure all of the systems are fixed until we know where they all are. The first thing most agencies had to do to prepare for the turn of the millennium was to create an inventory of all computer systems, and then to assess the risk posed by the failure of each of those systems. It is a commentary on computer security that no such inventory existed. The same situation applies to security. Before an agency can determine its risks, it must first create an inventory of all systems. Very few agencies have kept the inventory current.

When we mark up this bill, I intend to offer an amendment that would first, require all agencies to maintain a current inventory of systems. Second, I will require that agencies develop and include in the security report, a plan that establishes a system whereby every system will be tested over a five year period. With a current inventory and scheduled testing, we will be closer to security being a routine and not a unique government function.

Again, thank you Chairman Horn for your persistence in keeping computer security on our agenda. It is a dry and arcane subject, and all too often we let those issues slide.

**Your diligence is a valuable service to Congress and to the administration.**