

# **Congresswoman Candice S. Miller**

Opening Statement

Committee on Government Reform

Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census

June 24, 2003

---

## **OPENING STATEMENT**

Thank you, Mr. Chairman.

In a post-September 11<sup>th</sup> environment, the Federal government has been forced to re-evaluate its security procedures. The logistics associated with such a task are vast, and today we focus on the security of Federal information systems.

There has been a long-held belief that there should be one oversight facilitator for the entire Federal government – a government Chief Technology Officer, in a sense. This idea may have some merit, in order to ensure a government-wide standardization and interoperability. However one thing is clear -- as technology continues to evolve at an astonishing rate, the government must not be left behind, utilizing technologies and systems designed for a different time and a different type of threat. For these reasons, I am pleased that you have called this hearing, Mr. Chairman, so that Congress has the opportunity to objectively evaluate security measures taken by Federal agencies.

To be quite frank, with the active measures that international terrorists are taking against our freedoms, I am concerned that certain federal agencies appear to be lax with their efforts to improve systems safeguards. Oversight reports by the General Accounting Office and the Office of Management and Budget frequently identify areas of concern and countless examples of Federal agencies in non-compliance with various laws and regulations related to systems security. If an individual forgets to staple his or her w-2 form to a tax return, then that person lives in fear that the I.R.S. is going to conduct an audit. But it appears that some Federal agencies are above the law – feeling no need to fulfill even administrative requirements.

Incomplete and inaccurate reports that are required of Federal agencies, the apparent inability of agencies to reach their own stated performance goals, and in many cases, the blatant and utter disregard of Federally-mandated requirements are just some of the issues we are facing in this regard. Since September 11<sup>th</sup>, Americans have stated in poll after poll that homeland security and the war against terror is the most important issue facing our great nation. But I am concerned that individuals within the Federal government – individuals that Americans trust to protect them and their children – do not seem to understand the nature of this cyber-threat.

However, in spite of the current problems, the government is faced with a historic opportunity. With the passage of the Government Information Security Reform Act and the e-Government Act of 2002, which includes the Federal Information Security Management Act, Federal agencies now have the tools and the necessary support to develop and implement substantial information security reform. There has been some successes as the government moves forward – the work being done at the Department of Commerce is a fine example – and those examples of success should be used as a model for other agencies. I look forward to working with the Chairman and other Members of the Subcommittee to assist agencies with their reform objectives.

Thank you.