April 3, 2006

Mr. Alan Paller
Director of Research
The SANS Institute
8120 Woodmont Avenue, Suite 205
Bethesda, MD 20814

Dear Mr. Paller:

The Federal government has become increasingly dependent on information technology and the Internet for functions ranging from mission critical to administrative support services, and the need to secure its systems has intensified in turn. Agencies' poor performance in this area prompted the Government Accountability Office to include government-wide information security on its high-risk list since 1997. Therefore, I drafted the Federal Information Security Management Act of 2002 (FISMA), to require agencies to protect themselves against the ever-changing scope of cyber threats.

FISMA is intended to require federal agencies to establish a comprehensive agency-wide risk-based approach to information security management, including elements such as risk assessments, risk management policies, security awareness training, periodic reviews, and annual independent evaluation. FISMA reinforces provisions from the Government Information Security Reform Act, requires agencies to establish a foundation for information security, and allows them the flexibility to adapt to the changing threat environment.

As the Committee on Government Reform concludes its evaluation of the FY 2005 FISMA reports from federal agencies, we are looking at ways to improve federal information security. Therefore, I read with interest your comments in a March 15, 2006, *Government Executive* article on FISMA. I understand that you doubt the effectiveness of FISMA and think the scope of the Act forces agencies to focus on the wrong areas, preventing them from adequately securing their systems. Moreover, you have publicly criticized FISMA in the past.

Given your experience working on information security issues at The SANS Institute, I am interested in discussing your concerns about the government's current information security management framework and hearing your constructive ideas for strengthening it.

I believe agencies that comply with FISMA are more secure. But I am not so naïve or stubborn as to think FISMA is a panacea, or that important improvements could not be made. Thus, I look forward to hearing from you.

Sincerely,

Tom Davis
Chairman