

TOM DAVIS, VIRGINIA,
CHAIRMAN

CHRISTOPHER SHAYS, CONNECTICUT
DAN BURTON, INDIANA
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
GIL GUTKNECHT, MINNESOTA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
CANDICE MILLER, MICHIGAN
MICHAEL R. TURNER, OHIO
DARRELL ISSA, CALIFORNIA
JON C. PORTER, NEVADA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
CHARLES W. DENT, PENNSYLVANIA
VIRGINIA FOXX, NORTH CAROLINA
JEAN SCHMIDT, OHIO
VACANCY

ONE HUNDRED NINTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051
TTY (202) 225-6852

<http://reform.house.gov>

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
BRIAN HIGGINS, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA

BERNARD SANDERS, VERMONT,
INDEPENDENT

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.

Mr. Alan Paller
April 3, 2006
Page Two

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,

A handwritten signature in black ink, reading "Tom Davis". The signature is stylized with a large, looped "T" and a cursive "Davis".

Tom Davis
Chairman