

TOM DAVIS, VIRGINIA,
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. MCHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATT, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH 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

www.house.gov/reform

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
JOHN F. TIERNEY, MASSACHUSETTS
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
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

Congressman Adam Putnam, Chairman



OVERSIGHT HEARING

March 16, 2004

“Information Security in the Federal Government: One Year into the Federal Information Security Management Act.”

STATEMENT BY ADAM H. PUTNAM, CHAIRMAN

This is the first oversight hearing conducted by this Subcommittee on IT security this year. Last year, we learned much about threats, vulnerabilities, new technologies and new strategies for addressing the important issue of information security. Since our last hearing on this topic, the only thing that has really changed is the urgency of the threat. While I think it may be fair to say that there might be more discussions taking place about these issues, the time for discussion and debate now yields to a more important requirement for ACTION. Every month virus and worm attacks are becoming more prevalent and more malicious. One recent report placed the worldwide mitigation costs for the month of February 2004 at \$83 billion. Some might say that number is over inflated... but even if it's off by half, the number is still staggering.

The cyber threat poses some very unique and difficult challenges. Our infrastructure and government systems can be attacked from anywhere... at any time. We know that various terrorist groups are very sophisticated...and becoming more so each day, not to mention government sponsored attacks. Our government has taken very dramatic steps

to increase our physical security, but protecting our information networks has not progressed commensurately...either in the public...or private sector. DHS is really just getting its feet on the ground in this arena, and while I acknowledge the efforts of the National Cyber Security Division, I will reiterate my concern that we are “collectively” not moving fast enough to protect the American people and the U. S. economy from the very real threats that exist today.

The privacy and security of the public remains at risk. The economic damage being done to our economy is significant. The magnitude of this – clearly -- is what makes this hearing so important, because government-wide we still are failing to adequately secure our networks. Government must be the leader, we must set the standard and we must do it now. The oversight by this Subcommittee will be commensurate with the threat: Ever increasing and aggressive.

In December of last year, the Subcommittee released the 2003 Federal Computer Security Score Card. It was the 4th year that Federal agencies were graded following the process started by former Congressman Stephen Horn. This past scorecard, for the first time, based grades on the criteria established by the Federal Information Security Management Act (FISMA).

Chairman Tom Davis, through his FISMA legislation as part of the historic E-Government Act of 2002, has laid the groundwork for better security and better reporting for the government’s computer systems. This year’s grades were based on the FISMA compliance reports that the agencies provided to Congress and the Office of Management and Budget in September of last year. OMB has worked hard to advance computer security at all the Federal agencies and we have consulted OMB on the development of the scorecard. I would also like to thank the GAO for their invaluable help in preparation of these grades. This year is an important grading year because for the first time we can accurately compare the agencies to a previous year because the grading elements provided an apples-to-apples comparison. .

- This year overall the Federal Government gets a grade of D. That’s a modest increase over the F the government received last year.
- For the first time, two agencies (The Nuclear Regulatory Commission and the National Science Foundation) have received A’s.
- 14 agencies have increased their grades this year, although a couple actually went backwards.
- Only five agencies have completed reliable inventories of their critical IT assets leaving 19 without reliable inventories. This is very troubling considering we are four years into this process and still we have far too many agencies with incomplete inventories. How can you secure what you don’t know you have? How can you claim to have completed a certification and accreditation process absent a reliable inventory of your assets...?

- The IGs of three agencies (DoD, Veterans Affairs, and Treasury) did not submit independent reports in a timely manner and that is a serious problem. I must stress the IG component of this equation is critically important. The independent verification is vital and particularly in light of the fact that there were significant differences between many of the agencies and their IGs. 7 agencies had difference of two grades or more with their IGs.
- 14 agencies are still below a C and eight received failing grades.

As we worked on these grades, there were some overriding themes that became apparent for the agencies with good grades vs. those with poor grades.

- A full inventory of their critical IT assets.
- Identified critical infrastructure and mission critical systems.
- A strong incident identification and reporting procedures.
- Tight controls over contractors.
- Strong plans of actions and milestones that serve as guides for finding and eliminating security weaknesses

The Nuclear Regulatory Commission and the National Science Foundation should be commended for their outstanding scores, as well as the Social Security Administration and the Department of Labor for their B pluses. And, while DHS had a failing grade we recognize the difficult reorganization that took place and we expect significant improvement next year.

To assist agencies, I have requested that each one of the 24 graded agencies come and meet with my staff to discuss their grade. So far, we have met with 14 agencies and the results are encouraging. We have seen a great deal of enthusiasm and willingness to do the hard work necessary. The agencies have also expressed thanks for the opportunity to discuss the work that they are doing and the grades with the Subcommittee.

I am encouraged that OMB, in the recently released FISMA report, and during Clay Johnson's testimony two weeks ago, stressed that there is an increased determination to hold agencies accountable for implementing FISMA. However, there is some clarification that I will seek today in something that was written in the OMB report. The report on page 13 says the following:

“While awareness of IT security requirements and responsibilities has spread beyond security and IT employees, more agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. This particular issue requires the Federal government to think of security in a new manner. The old thinking of IT security as the responsibility of a single agency official or the agency's IT security office is out of date, contrary to law and policy, and significantly endangers the ability of agencies to safeguard their IT investments.”

While I certainly agree that IT security is certainly a collective responsibility the language I referred to seems to indicate that no one person can be held accountable. I

disagree. This Chairman and this Subcommittee will seek accountability of the highest agency official responsible for information technology investments to insure that IT Security is baked into the investment decision making process, consistent with the law as established by the Clinger-Cohen Act. In fact, I have already initiated a process, working with Chairman Davis, to amend the Clinger-Cohen Act to explicitly identify information security as a required element of the IT investment management oversight and decision making process within every agency of the federal government. The grade of D for the Federal Government is simply not acceptable.

Quite frankly, one of the continuing impediments to progress is that too many people still view information security as a technology issue. This is a management and governance issue and must be accounted for in every business case and in implementation of a federal enterprise architecture. This must be the responsibility of all stakeholders and the silo walls must come down with this and other transformation efforts to employ collaborative solutions that will provide increased safety and protection for the American people and the U. S. economy.

I welcome and applaud the increased oversight being employed by the Office and Management and Budget through the use of existing tools and business case evaluation. I especially applaud the recent pronouncement that OMB will not approve agency expenditures for IT development and modernization projects until they have sufficiently demonstrated that their existing information technology assets are secure. Working together as “partners in progress”, we will continue to be vigilant in our efforts to achieve the security of the information networks that support the mission activities of the federal government, and protect the information assets that they contain.

To assist agencies in identifying and selection such technologies, I have asked GAO to categorize specific technologies according to the functionality they provide and describe what the technologies do, how they work and their reported effectiveness. GAO is releasing this report today and I want to thank them for their work and effort in producing this important product

I would like to welcome all our witnesses here today. Thank you for your time and I look forward to your testimony.

###