Uncle Sam Gets a C-Minus for Information Security

April 13 2007

A report by a House committee on FISMA compliance gives the federal government a C-minus in its efforts to protect data on its computer systems.

A House committee gave the federal government a grade of C-minus for 2006 as part of the committee's annual assessment of how well information is protected on government computers.

The annual report by the House Government Oversight and Reform Committee is meant to judge compliance with the Federal Information Security Management Act. The committee has given the government overall grades of D, D-plus and D-plus in 2003, 2004 and 2005, respectively.

Rep. Tom Davis (R-Va.), a ranking member of the committee, said the grade indicates a slight improvement.

"Obviously, challenges remain," Davis said in a statement. "While there are some excellent signs of progress in this year's report, and that's encouraging, I remain concerned that large agencies like the U.S. Dept. of Defense and the U.S. Department of Homeland Security are still lagging in their compliance."

The U.S. Department of Justice and the U.S. Department of Housing and Urban Development showed the most improvement from 2005 to 2006. The DOJ jumped from a D to an A-minus, while HUD climbed from D-

plus to A-plus. HUD, for the first time, developed a full inventory of its information security apparatus, which the committee counted as a major plus in the grading.

NASA fell from a B-minus to a D-minus, and the Department of Education dropped from a C-minus to an F, according to the committee.

The grades are derived from annual reports that agencies produce to comply with FISMA (Federal Information Security Management Act). Agencies are rated on their annual tests of information security, their plans of action and how they detect and react to breaches of security.

The Department of Homeland Security received a D for 2006, marking the first time it did not receive an F since ratings began in 2003. Davis called the DHS' establishment of an inventory of its secure computer systems a critical first step to information security.

"You can't protect what you don't know you have," Davis said.

Philip M. Heneghan, chief information security officer at USAID (U.S. Agency for International Development), credited the agency's executive leadership for setting the tone that has allowed the organization to receive consistently high grades. USAID was among eight agencies to score between an A-minus and an A-plus for 2006.

"We stress the importance of people, process and technology," he said. "Wherever possible, we've automated parts of our FISMA program. For example, we developed security awareness training software that provides training to all 8,000-plus USAID network users before they are allowed to get on our network."

Khalid Kark, a senior analyst at Forrester in Cambridge, Mass., said compliance does not always equal security.

"The perception is if you get a D or an F you can be hacked," he said. "That's not true."

The Department of Defense for example does a good job of protecting sensitive data, he said, and probably cannot share all of its practices.

In addition, when it comes to compliance, size matters.

"The bigger you are, the harder it is to coordinate that effort, to coordinate all those resources," Kark said, adding that the DOD is composed of some 2.7 million people.

Still, Jeremy Nazarian of Lumeta, based in Somerset, N.J., said the grading system is a decent measure of how compliant an organization is with security policies defined by the National Institute of Standards and Technology.

Lumeta provides network assurance tools to IT organizations so they can track network change over time and ensure that their security policies and their network architecture remain aligned.

"Like most exercises that involve letter grading, the score is not necessarily a complete representation of how an agency is doing," said Nazarian, Lumeta's vice president of marketing.

"For example, agencies are under pressure to deliver applications in support of e-Gov and to modernize their architectures. This kind of change often affects security posture adversely, and is a mitigating circumstance that doesn't show up in the score. However, organizations that have the ability to measure the impact of change on risk will be able to take on hard projects and not see their scores decline," Nazarian said.

Davis said he is exploring ways to provide an incentive through the

scorecard process to agencies that effectively configure their systems with security in mind. For example, as agencies move to Microsoft Vista, bonus points could be awarded to agencies that take certain steps toward secure configurations.

Alan Paller, director of research for the SANS Institute in Bethesda, Md., said in a statement that the idea of incentive points opens the door to huge improvements in federal information security.

"It could have a profound effect if changes in congressional focus and grading provide the necessary incentive to persuade agencies to implement the new OMB-mandated secure configurations faster and more broadly," Paller said.