



House intel panel 'conditionally supports' cyber effort

By JOHN T. BENNETT
July 29, 2008

A powerful House panel has given its "conditional support" to President Bush's new unprecedented cyber security initiative, despite its concerns about cost and government-industry collaboration.

The White House's 2009 budget package asked Congress to provide billions of dollars for a new program to fortify crucial U.S. governmental and private-sector networks.

In a little-noticed report released earlier this summer, the House Permanent Select Committee on Intelligence wrote that it "believes a cyber security initiative worthwhile in principle, but the details of the [program] remain vague and, thus, open to question."

The reports continues: "Until some of the governance, implementation, and policy issues are identified, debated, and resolved, the Committee believes that the funding request is excessive."

The amount the White House requested is classified, according to sources.

One defense official said the program would cost \$16 billion over five years; other defense-sector sources peg the number at more than \$30 billion.

In recent years, the panel's report said, the cyber threat "has continued to grow in scale and sophistication." The report calls the president's plan "reasonable," yet says the committee "remains concerned about program management and systems engineering capabilities" across the government.

The lawmakers also reveal their worries about the ability of the federal government and private sector to work together to shore up key U.S. public and private networks.

"For the [cyber program] to work as described in the presidential directive, it will require a partnership with industry unlike any model that currently exists," the report said. "The excessive classification of the CNCI, however, militates against the collaboration necessary to achieve that partnership."

Government agencies may also conflict about how to implement the program.

"The Committee also notes that the federal government is not presently organized or equipped to negotiate the myriad issues and challenges presented by the implementation of the CNCI, especially those that cross organizational and jurisdictional boundaries," the lawmakers wrote.

The panel notes many of the components that will be a part of the national cyber security system "do not seem very well-connected, nor is it clear there are adequate governance mechanisms to achieve the necessary coordination."

Sources said the U.S. intelligence Community, Defense Department and Department of Homeland Security will play central roles in the new initiative.

But since word of the new program became public early this year, there have been whispers in Washington that the White House has provided Congress and federal officials too few details about how departments should implement the program.

Within the Pentagon, the effort to develop guidance that will spell out the military's role in the new program is being led by Paul McHale, the assistant secretary of defense for homeland defense.

Bush administration officials have called the program "very classified" and feel more needs to be done to steel U.S. networks against the kind of debilitating strike that paralyzed Estonian servers for several days last spring. Another threatened the Pentagon this year, and may have been launched from China. Congressional offices also have reported attacks on their computer systems.

Some Pentagon officials have said publicly the U.S. and its allies essentially are already at war in cyberspace with a range of enemies.