US Advisory panel recommends more federal R&D spending

By *srlinuxx*
Created *19/03/2005 - 2:26pm*
Submitted by srlinuxx on Saturday 19th of March 2005 02:26:34 PM Filed under Security [1]

The Presidential IT Advisory Committee (PITAC) has recommended the federal government sharply increase its spending on cybersecurity R&D and shift the focus to fundamental, long-term solutions to security challenges.

"The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects," PITAC warned in a letter submitting the report, titled Cyber Security: A Crisis in Prioritization, to the president. "These vulnerabilities put the nation's entire critical infrastructure at risk."

Current practices of patching vulnerabilities as they are found address immediate needs, but the committee concluded that "fundamentally different architectures and technologies are needed so that the IT infrastructure as a whole can become secure."

The government has a vital role to play in supplying the intellectual capital to improve IT security, PITAC said, but in recent years its focus increasingly has been on short-term problems addressing the needs of the military and intelligence communities. The results too often are classified, and more effort is needed to transfer them into the mainstream market.

The advisory committee examined funding for basic research by the National Science Foundation, the Defense Advanced Research Projects Agency, the Homeland Security Department, the National Security Agency, and the National Institute of Standards and Technology.

NSF, with its $30 million Cyber Trust program, is the primary source of funds for civilian security research. PITAC recommended that the program be expanded by at least $90 million annually.

The $5.47 billion NSF appropriation for fiscal 2005, approved by Congress in November 2004, is more than $60 million less than fiscal 2004 funding, and $227 million less than requested by the president.

PITAC recommended that:

- NSF R&D funding be increased by at least $90 million a year, while also substantially increasing funding for DARPA and DHS.
- Government increase efforts to expand the number of cybersecurity experts in the academic community, doubling the number by the end of the decade. The committee estimates there are fewer than 250 cybersecurity specialists working now.

- Security technology transfer programs be strengthened to speed the introduction of needed off-the-shelf tools and technologies into the marketplace. The government should sponsor an annual interagency conference to showcase the results of cybersecurity R&D.
- The Interagency Working Group on Critical Information Infrastructure Protection should coordinate federal R&D efforts and be integrated under the Networking and Information Technology Research and Development Program.

The committee identified 10 critical areas for future research:

- Computer authentication methodologies, so sources of packets can be traced in large-scale networks
- Secure fundamental networking protocols
- Secure software engineering
- End-to-end system security, rather than merely secure components
- Monitoring and detection to quickly identify problems
- Mitigation and recovery methodologies to avoid catastrophic failure when problems occur
- Cyberforensics tools for aid in criminal prosecutions
- Modeling and test beds for new technologies
- Metrics, benchmarks and best practices for evaluating the security of security products and implementing them
- Nontechnical societal and government issues.

Article on gcn.com [2].

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://www.gcn.com/vol1_no1/daily-updates/35311-1.html