

Wanted: Computer hackers... to help government

April 19 2009, By LOLITA C. BALDOR , Associated Press Writer



Barack Obama tucks a paper into his suit jacket after delivering a speech during the opening session of the 5th Summit of the Americas in Port of Spain, Trinidad and Tobago, Friday April 17, 2009. In the background are Chile's President Michelle Bachelet, left, and Brazil's President Luiz Inacio Lula da Silva. (AP Photo/Andres Leighton)

(AP) -- Wanted: Computer hackers. Federal authorities aren't looking to prosecute them, but to pay them to secure the nation's networks.

General Dynamics Information Technology put out an ad last month on behalf of the Homeland Security Department seeking someone who could "think like the bad guy." Applicants, it said, must understand hackers' tools and tactics and be able to analyze Internet traffic and

identify vulnerabilities in the federal systems.

In the Pentagon's budget request submitted last week, Defense Secretary Robert Gates said the Pentagon will increase the number of cyberexperts it can train each year from 80 to 250 by 2011.

With warnings that the U.S. is ill-prepared for a cyberattack, the White House conducted a 60-day study of how the government can better manage and use technology to protect everything from the [electrical grid](#) and stock markets to tax data, airline flight systems, and nuclear launch codes.

President Barack Obama appointed a former Bush administration aide, Melissa Hathaway, to head the effort, and her report was delivered Friday, the White House said.

While the country had detailed plans for floods, fires or errant planes drifting into protected airspace, there is no similar response etched out for a major computer attack.

David Powner, director of technology issues for the Government Accountability Office, told Congress last month that the U.S. has no recovery plan for a digital disaster.

"We're clearly not as prepared as we should be," he said.

Administration officials says the U.S. has not kept pace with technological innovations needed to protect its computer networks against emerging threats from hackers, criminals or other nations looking for national security secrets.

U.S. computer networks, including those at the Pentagon and other federal agencies, are under persistent attack, ranging from nuisance

hacking to more nefarious assaults, possibly from other nations, such as China. Industry leaders told Congress during a recent hearing that law enforcement and other protections are too outdated to fend off threats from criminals, terrorists and unfriendly foreign nations.

Just last week, a former government official revealed that spies had hacked into the U.S. electric grid and left behind computer programs that would let them disrupt service. The intrusions were discovered after electric companies gave the government permission to audit their systems, said the ex-official, who was not authorized to discuss the matter and spoke on condition of anonymity.

Cyberthreats are also included as a key potential national security risk outlined in a classified report put together by Adm. Mike Mullen, chairman of the Joint Chiefs of Staff. Pentagon officials say they spent more than \$100 million in the last six months responding to and repairing damage from cyberattacks and other computer network problems.

Nadia Short, vice president at General Dynamics Advanced Information Systems, said the job posting for ethical hackers fills a critical need for the government.

The analysts keep constant watch on the government networks as part of a program called Einstein that was initiated by the Bush administration under the U.S. Computer Emergency Readiness Team.

Short said the \$60 million, four-year contract with US-CERT uses the ethical hackers to analyze threats to the government's computer systems and develop ways to reduce vulnerabilities.

Faced with such cyberchallenges, Obama ordered the 60-day review to examine how federal agencies manage and protect their massive amounts

of data and what the government's role should be in guarding the vast networks that control the country's vital utilities and infrastructure.

Over the past two months, Hathaway met with hundreds of industry leaders, Capitol Hill staff and other experts, seeking guidance on what the federal government's role should be in protecting information networks against an attack. She sought recommendations on how officials should define and report cyberincidents and attacks; how the government should structure its cyberoversight; and how the nation can increase security without stifling innovation.

A task force of technology giants, including representatives from General Dynamics, IBM, Lockheed Martin and Hewlett-Packard Co. urged the administration to establish a White House-level official to lead cyberefforts and to develop ways to share information on problems more quickly with the private sector.

The administration has struggled with the basics, such as who should control the nation's cyberspace programs. There appears to be some agreement now that the White House should coordinate the overall effort, rejecting suggestions that the National Security Agency take it on - a plan that triggered protests on Capitol Hill and from civil liberties groups worried about giving such control to spy agencies.

On the Net:

White House: <http://www.whitehouse.gov>

General Dynamics Advanced Information Systems: <http://www.gd-ais.com/>

U.S. Computer Emergency Readiness Team: <http://www.us-cert.gov/>

GAO report: <http://tinyurl.com/aczgk6>

©2009 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Wanted: Computer hackers... to help government (2009, April 19) retrieved 19 September 2024 from <https://phys.org/news/2009-04-hackers.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.