

BusinessWeek

TECHNOLOGY September 15, 2008, 7:06PM EST

U.S. Cybersecurity Is Weak, GAO Says

The Government Accountability Office says the team responsible for protecting private- and public-sector computers isn't up to snuff

by [Keith Epstein](#)

The federal government cybersecurity team with primary responsibility for protecting the computer networks of government and private enterprise isn't up to the job, according to a draft Government Accountability Office [report](#) obtained by *BusinessWeek*.

The U.S. Computer Emergency Readiness Team, known as US-CERT, mans the front line in any cyber-attack. The group monitors computer networks for hacker threats, investigates suspicious activity online, and is supposed to issue timely alerts to information technology security professionals from the White House to corporations and electric utilities. But the GAO draft report describes US-CERT as bedeviled by frequent management turnover, bureaucratic challenges that prevent timely sounding of alarms, a lack of access to networks across wide swaths of critical terrain, and an inability to fill large numbers of positions with qualified workers.

Five years after the Homeland Security Dept. took charge of the team as a critical safeguard against threats to national security, US-CERT "still does not exhibit aspects of the attributes essential to having a truly national capability," according to the draft report.

VULNERABLE TO FOREIGN ADVERSARIES

Privately, many within government and industry have grown increasingly concerned about the lack of such a capability. Without being able to effectively monitor a wide variety of computer networks across the country and quickly issue warnings of possible attacks, the government is, in effect, flying blind, or at least partially blind, despite the best of intentions. As [BusinessWeek reported in April](#) (*BusinessWeek*, 4/10/08), the concern these days is not merely that a pimply teenager in Bratislava will hack a corporate network or that Russian hackers will shut down a retailer's Web site with a so-called "denial-of-service attack." Rather, it's that there could be a sophisticated intrusion of sensitive computer networks by a potential foreign adversary such as China.

An independent bipartisan commission of corporate executives, network security specialists, and military and intelligence officials plans to go public with its concerns about the issue. "The central problems," James Lewis, a technology analyst at the Center for Strategic & International Studies, plans to tell Congress in testimony prepared for hearings on Sept. 16, "are the lack of a strategic focus, overlapping missions, poor coordination and collaboration, and diffuse responsibility."

A series of troubling intrusions in recent years, grouped under code names such as Byzantine Foothold and Titan Rain, were not initially recognized as being connected. They caused anxiety at major agencies of the federal government and among big defense contractors such as Boeing ([BA](#)) and Lockheed Martin ([LMT](#)).

GOALS NOT BEING MET

The importance of recognizing patterns of attack across a broad swath of cyberspace is now accepted at the highest levels of the military, intelligence, political, financial, and industrial communities. Worries range from attacks on electric power plants to the potential for using computer networks to undermine a financial institution's viability. Thefts of funds by sophisticated hackers are now routine occurrences around the world.

But recognizing the larger pattern requires the people, technology, and access to sift through huge amounts of suspicious activity, and in its draft report the GAO has evidently concluded the envisioned goal is not being met.

In one of the report's more critical passages, the GAO finds that US-CERT "lacks a comprehensive baseline understanding of the nation's critical information infrastructure operations, does not monitor all critical infrastructure information systems, does not consistently provide actionable and timely warnings, and lacks the capacity to assist in mitigation and recovery in the event of multiple, simultaneous incidents of national significance."

Homeland Security officials say their difficulties should come as no surprise; it's a huge mission. Says DHS spokesman Laura Keehner: "We are undertaking something not unlike the Manhattan Project. We have set a strong cyber strategy, recently created the National Cyber Security Center, and are in the process of aggressively hiring several hundred analysts to further our mission of securing critical infrastructure. Billions of dollars are going into this effort. We're the first to admit there is more work to be done; we are focused on collaborating with the private sector—which owns the vast majority of this country's critical infrastructure—to mitigate threats."

READY TO "RAMP UP"

The Homeland Security Dept.'s top official overseeing national cybersecurity efforts, Robert Jamison, seems to agree with at least some of the shortcomings. "We need comprehensive, consistent intrusion detection," Jamison told a network security industry group on Sept. 15. He told members of the Information Technology Assn. of America that more also needed to be done to protect the networks of corporations, and urged people to apply for jobs to "help us ramp up and meet the challenges."

In January 2008, President Bush signed directives launching an expensive and theoretically expansive national cybersecurity initiative. Many of its provisions are classified, but *BusinessWeek* detailed [the main points](#) in April (*BusinessWeek*, 4/10/08).

Central to the realization of the plan to bolster national security in cyberspace: A more powerful US-CERT.

ACTIONS ARE INADEQUATE

For the government, one cornerstone of the effort is supposed to be creation of a real-time intrusion detection monitoring system throughout the government, with the moniker "Einstein." The idea: to make everything, every piece of data, every attempted entry, or removal of data, visible to the team of monitors at US-CERT.

But the GAO draft report says that the weaknesses in the security effort are so significant that building tools such as Einstein or hiring 80 new cyber-analysts may not be sufficient. "It is unclear whether these actions will help US-CERT—or whatever organizational structure is ultimately charged with coordinating national cyber-analysis and warning efforts—achieve the objectives" of the national cybersecurity initiative, the report says.

Concludes the GAO: Homeland Security's actions to address US-CERT's weaknesses "have not been adequate."

WEAK WARNING CAPABILITIES

Homeland Security, in a July 3 response that is part of the draft GAO report, agreed with many of the GAO's conclusions but said it was making improvements. An expanded program known as "Einstein 2," it said, will help US-CERT "maintain situational awareness" around the clock. "Einstein 2 will alert when specific malicious network activity is detected and provide US-CERT with increased insight into the nature of that activity."

At the same time, Homeland Security, in its response, took issue with criticism that its warnings came too late. "We do not agree with the report's repeated description of US-CERT's warnings and notifications are 'not consistently actionable or timely,'" wrote Jerald Levine, director of a division of the office of the Homeland Security Dept. inspector general.

Among GAO's criticisms were "a number of newly identified and ongoing challenges that impede it from fully

implementing the key attributes and in turn establishing cyber-analysis and warning capabilities essential to coordinating the national effort to prepare for, prevent, and respond to cyberthreats."

ADVISING THE NEXT PRESIDENT

The GAO isn't the only critic of the nation's existing cyberdefenses. Lewis is part of an independent commission created to make recommendations on computer security for the next President. "Cybersecurity is now one of the most important national security challenges facing the U.S.," he says, according to his prepared Congressional testimony. "This is not some hypothetical catastrophe. We are under attack and taking damage." Despite a Bush Administration cybersecurity initiative, adds Lewis, "the U.S. is not organized and lacks a coherent national strategy" for addressing cyberthreats.

The commission has concluded that "none of the existing cybersecurity structures are adequate," Lewis says, according to his testimony, including "central problems in the current federal organization for cybersecurity." "Much of the problem," Lewis goes on, "resides with the performance and capabilities of the Department of Homeland Security."

Recommendations of the bipartisan commission, whose members include corporate executives, members of Congress, scientists, network security experts, and military and national security officials, are to be made public in November. Lewis is to testify before the House Committee on Homeland Security's subcommittee on emerging threats, cybersecurity, and science and technology.

[Epstein](#) is a correspondent in BusinessWeek's Washington bureau.

Xerox Color. It makes business sense.

Copyright 2000-2008 by The McGraw-Hill Companies Inc. All rights reserved.

The McGraw-Hill Companies