ROLL CALL

Security Program Has Gaps

March 15, 2010
By Emily Yehle
Roll Call Staff

Capitol Police officials are requiring some of their employees to use a contractor's online program to list Congress' security deficiencies, leaving open the possibility of hackers gaining access.

The program — managed by contractor M.C. Dean — lists the ongoing status of security equipment throughout the Capitol complex. Employees enter their "work orders" into the system, describing the nature, location and status of a security deficiency that they are tasked with fixing. Each work order focuses on one issue, such as a damaged barrier or malfunctioning camera in a Congressional building.

But the program appears to have several security flaws, including simple passwords and the fact that employees can log in to the program on their personal computers at home. The House Administration Committee and the House Appropriations Subcommittee on the Legislative Branch are investigating the issue, according to the committees' spokesmen.

"The safety and security of the Capitol Complex and the Members, Staff and Visitors are of primary importance to the Committee," Kyle Anderson, spokesman for House Administration Chairman Robert Brady (D-Pa.), said in an e-mail. "To that end, we are looking into the issue and will explore next steps based upon our findings."

Capitol Police Chief Phillip Morse declined to be interviewed, but department spokeswoman Sgt. Kimberly Schneider sent an e-mail confirming that M.C. Dean's system is used to track maintenance activities for the department's "security management system, and for budget preparation and formulation."

But she said the system — the Infrastructure Maintenance Management System — is also used by agencies such as the Library of Congress and departments in the Army, Navy and Air Force. It is hosted by a computer server that is in a secure room monitored by security cameras, she said.

"Additionally, access to the data itself is controlled many ways; traditional software firewalls are in place, a Secure Socket Layer (SSL) communications protocol exists to encrypt (128 bit) network traffic between the server and client computers, as well as traditional user level protections such as layered access levels and user log-in/password protection," she said in the e-mail. "The network to the server is protected by a network intrusion detection system and alarms (detecting network 'hack' attempts) are monitored 24/7."

Anderson wouldn't go into details on what aspects of the online system the House Administration Committee is concerned about, but outside experts say the nature of the system raises some questions about whether the level of security is adequate. The issue, they say, is whether the security system is off-the-shelf or actively monitored and tailored to the Capitol Police's level of risk.

"There are some elementary and obvious problems, but there also may be some that are deeper still that would be revealed in a deeper audit," said Gene Spafford, a computer security expert at Purdue University.

Spafford, who did not work on the system or see it firsthand, said putting sensitive information on an online system opens it up to a world full of hackers, viruses and spyware. That risk is heightened, he said, when employees can access the system on the same personal computers that they use to view videos, check personal e-mail and surf the Web.

Add a simple alphanumeric password, he said, and there is a "nonzero chance" that an unauthorized person could access the database.

On systems such as these, “one of the obvious difficulties is that the authentication to get access is incredibly weak. It is susceptible to having passwords intercepted or guessed and reused by others,” he said, later adding, “All they need to get in is an account, a name and an obvious password.”

Jim Lewis, director of the technology and public policy program at the Center for Strategic and International Studies, agreed that the simple password was a security risk, but he said using an online system is cheap, efficient and can be the best choice. Just requiring users to have more complex passwords would help beef up the security, he said.

“The traditional problem is that this online stuff is much more efficient,” he said. But, he added, “if you don’t think about security, it makes you much more vulnerable.”

Schneider confirmed that employees can access the IMMS system at home but said security risks are “eliminated” because the contractor requires “access level restrictions” or restricts the amount of information seen depending on the employees’ clearance level. She also said the system was encrypted and “password protected,” but she declined to detail the level of difficulty of such passwords.

The IMMS system is used by the Capitol Police’s Security Services Bureau, a division that handles the design, implementation and maintenance of the security equipment in and around the Capitol and Congressional buildings. Among other things, that includes communications equipment, security systems and the Sensitive Compartmented Information Facilities where Members read classified documents.

According to a recent internal document, supervisors in the bureau’s Security Equipment Section require employees to complete about four work order tickets in the online system each day in order to get a successful performance review. Among the reasons: justification for the division’s budget and progress reports to Morse.

Several knowledgeable sources say such a quota encourages employees to get creative with their work orders. For example, if an employee is working on one serious problem that may take days, he might split it up into several work order tickets to avoid a reprimand.

But concerned employees have little recourse to object to the system. The Office of Compliance has ruled that they cannot enter a bargaining unit because of the “nature of the work performed,” Schneider said. Thus, employees can use only the internal complaint system, which sends complaints to the same supervisors requiring employees to use the system.

The online system also raises questions about the management of the Security Services Bureau and its relationship to M.C. Dean. According to several knowledgeable sources, two supervisors in the Security Equipment Section were forced to resign a couple years ago after showing homosexual pornography to their employees. Soon after, sources say, both were hired at M.C. Dean.

M.C. Dean officials did not return calls for comment, but the two supervisors were on the payroll of the House Capitol Police Board until 2003, when the payroll responsibilities were handed to the Capitol Police (which doesn’t have public records of its employees). Calls to M.C. Dean confirmed that two employees with the same names as the supervisors work for the security contractor.

Schneider said the department does not discuss personnel issues, but that the supervisors no longer work for the Capitol Police and such allegations are “not factual.”

But M.C. Dean appears to be very involved in the Capitol Police’s security infrastructure. A retired Capitol Police detective said that while he was in the department, he noticed that M.C. Dean contractors were tasked with working on sensitive security systems while highly trained Capitol Police employees were often sent to do menial jobs.

“I just never understood why they hired so many people — talented people — for physical security, put them through all the training, made them part of the United States Capitol Police and then all of the sudden just told them, ‘You don’t touch this, you don’t touch that. Only M.C. Dean does,’” he said. “I don’t understand it at all.”

Schneider confirmed that M.C. Dean contractors “perform installation, maintenance, and service work on the electronic security systems” in order to ensure that the system works 24/7. But not all those employees have security clearance, though they go through the “standard USCP background check.”

“Additionally,” she said, “each M.C. Dean functional specialty group does have at least one individual who is cleared to the [Top Secret/Sensitive Compartmented Information] level to support work” on Sensitive Compartmented Information Facilities.