The National Journal

August 19, 2011

Investigation Reveals Widespread Insider Hacking at Immigration Agency

BYLINE: Aliya Sternstein

A yearlong probe into computer fraud at an immigration-application processing center uncovered multiple incidents of internal hacking where staff accessed management-level e-mails and other confidential files, according to Homeland Security Department interviews, network analyses, and internal e-mails obtained byem.

The investigation began in January 2008, when officials at U.S. Citizenship and Immigration Services, which is part of Homeland Security, reported to the department's inspector general that numerous employees had violated federal security rules at the agency's Texas Service Center, one of four regional centers that handle a variety of immigration-related petitions and applications. According to the materials obtained, employees and supervisors abused system logon privileges, gained unauthorized access in some instances, and then allegedly sabotaged audit logs to leave behind no traces of their illicit activities. IG papers list the redacted names of 17 subjects of the investigation, all of whom were information-technology specialists.

The evidence of breaches at the center is the latest revelation of insider threats at USCIS. With their ill-gotten access, the Texas personnel were capable of, for example, granting citizenship rights, as well as reading files containing sensitive information on contract awards, immigration reform or other policy formulations, say former USCIS IT officials there at the time.

Federal agents located so-called hackware in several computer drives -- software that lets users intercept business information passing through the agency's network, according to one investigative analysis signed in March 2008.

In another instance, a staffer in a position of authority asked for the logins and passwords of all software and systems at the service center, which would have granted that person unauthorized access to all goings-on at the facility.

A November 27, 2007, e-mail from the manager with the subject line: "FW: TSC Logins and passwords." The body of the e-mail stated: "I will need the administrator password for every piece of hardware in the TSC that requires a password. I will also need the administrator password for any enterprise type software that has an administrator password." The manager then said, "Please do not send them in e-mail unless you encrypt the text file" -- or scramble the data to render it unreadable. "You can call me to provide the encryption password."

Federal computer fraud laws prohibit the unauthorized use of administrator passwords, the former IT managers said.

Separately, an employee told agents that a few federal IT specialists had acquired prohibited codes for reading other center employees' e-mails -- authorizations dubbed "God rights," according to an interview report signed February 2008. The employee "related that [Texas Service Center] IT employees should not have had enterprisewide rights (commonly referred to as 'God' rights) because it was a restricted administrative status that was reserved for CIS [Office of Information Technology] upper management," the write-up stated.

The U.S. Attorney's Office for the Northern District of Texas declined to criminally prosecute the subjects of the investigation for computer fraud, according to the inspector general's materials obtained.

An IG memo stamped October 1, 2008, stated that the final investigation was delivered to Jan Lane, chief of the USCIS Office of Security and Integrity, so that the agency could take whatever disciplinary action it deemed appropriate.

Agency officials would not comment on the outcome of the case, and Lane no longer works there. They said in a statement, "USCIS demands that our employees maintain the highest ethical standards. When allegations of misconduct are made, USCIS takes immediate action to protect the integrity of the workplace and to ensure that the facts are investigated fully. USCIS is committed to taking full and appropriate disciplinary action against any employee who is found to have violated our standards."

Recent years have seen a number of documented cases where employees or contractors tampered with secure IT systems. Government investigators have warned that the agency could become more vulnerable to insider threats because designs for a current IT overhaul do not include protections against such activities.

For example, a 2008 serious incident report obtained byemshows that USCIS officials discovered internal wrongdoing at a Vermont processing center. The records show that employees within the Fraud Detection and National Security Directorate -- hired to ensure dangerous individuals are not accorded legal status -- hooked up a nongovernment computer to an external Internet connection, potentially allowing them to import or export data for committing identity theft.

More recently, a former USCIS contractor was sentenced to five and a half years in jail for falsifying files to help illegal immigrants receive "legal" passports. Justice Department officials announced the punishment in late May, after Richard Abapo Quidilla, 39, of Pico Rivera, Calif., pleaded guilty to computer fraud, among other charges. He deleted the names, birth dates, and other personal data of naturalized citizens in a secure database and substituted the corresponding information of illegal immigrants, according to federal district court papers.

The agency could open itself up to greater risk of insider wrongdoing because of poor planning for an ongoing $2.4 billion project to automate immigration paperwork, IG officials reported in

January. USCIS Transformation, the online system that is supposed to improve fraud detection, is missing controls to prevent internal hacking, according to the audit.

Frank Deffer, assistant IG for information-technology audits, wrote that based on a "review of the requirements for fraud detection and national-security issues, it appears there are no requirements to address insider threats" to Transformation. "Insiders at USCIS have perpetrated fraud in the past" and internal staff "are capable of granting legal residency or citizenship status to someone who poses a national security risk to the United States," he added.