Security contractor breach not detected for months

November 3 2014, by Stephen Braun

In this photo taken Oct. 17, 2014, the USIS building in Falls Church, Va. A cyber-attack similar to previous hacker intrusions from China penetrated computer networks for months at USIS, the government's leading security clearance contractor, before the company noticed the break-in, officials and others familiar with an FBI investigation and related official inquiries told The Associated Press. The breach compromised the private records of at least 25,000 employees at the Homeland Security Department and cost the company hundreds of millions of dollars in lost government contracts. (AP Photo/J. Scott Applewhite)

A cyberattack similar to previous hacker intrusions from China penetrated computer networks for months at USIS, the government's leading security clearance contractor, before the company noticed, officials and others familiar with an FBI investigation and related official inquiries told The Associated Press.

The breach, first revealed by the company and government agencies in August, compromised the private records of at least 25,000 employees at the Homeland Security Department and cost the company hundreds of millions of dollars in lost government contracts.

In addition to trying to identify the perpetrators and evaluate the scale of the stolen material, the government inquiries have prompted concerns about why computer detection alarms inside the company failed to quickly notice the hackers and whether federal agencies that hired the company should have monitored its practices more closely.

Former employees of the firm, U.S. Investigations Services LLC, also have raised questions about why the company and the government failed to ensure that outdated background reports containing personal data weren't regularly purged from the company's computers.

Details about the investigation and related inquiries were described by federal officials and others familiar with the case. The officials spoke only on condition of anonymity because they were not authorized to comment publicly on the continuing criminal investigation, the others because of concerns about possible litigation.

A computer forensics analysis by consultants hired by the company's lawyers defended USIS' handling of the breach, noting it was the firm that reported the incident.

The analysis said government agencies regularly reviewed and approved

the firm's early warning system. In the analysis, submitted to federal officials in September and obtained by the AP, the consultants criticized the government's decision in August to indefinitely halt the firm's background investigations.

In this photo taken Oct. 17, 2014, the USIS building in Falls Church, Va. A cyber-attack similar to previous hacker intrusions from China penetrated computer networks for months at USIS, the government's leading security clearance contractor, before the company noticed the break-in, officials and others familiar with an FBI investigation and related official inquiries told The Associated Press. The breach compromised the private records of at least 25,000 employees at the Homeland Security Department and cost the company hundreds of millions of dollars in lost government contracts. (AP Photo/J. Scott Applewhite)

USIS reported the cyberattack to federal authorities on June 5, more than two months before acknowledging it publicly. The attack had hallmarks similar to past intrusions by Chinese hackers, according to

people familiar with the investigation. Last March, hackers traced to China were reported to have penetrated computers at the Office of Personnel Management, the federal agency that oversees most background investigations of government workers and has contracted extensively with USIS.

In a brief interview, Joseph Demarest, assistant director of the FBI's cyber division, described the hack against USIS as "sophisticated" but said "we're still working through that as well." He added: "There is some attribution" as to who was responsible, but he declined to comment further.

For many people, the impact of the USIS break-in is dwarfed by recent intrusions that exposed credit and private records of millions of customers at JPMorgan Chase & Co., Target Corp. and Home Depot Inc. But it's significant because the government relies heavily on contractors to vet U.S. workers in sensitive jobs. The possibility that national security background investigations are vulnerable to cyber-espionage could undermine the integrity of the verification system used to review more than 5 million government workers and contract employees.

"The information gathered in the security clearance process is a treasure chest for cyber hackers. If the contractors and the agencies that hire them can't safeguard their material, the whole system becomes unreliable," said Alan Paller, head of SANS, a cybersecurity training school, and former co-chair of DHS' task force on cyber skills.

Last month, the leaders of the Senate Homeland Security and Governmental Affairs Committee, Tom Carper, a Democrat, and Tom Coburn, a Republican, pressed OPM and DHS about their oversight of contractors and USIS' performance before and during the cyberattack.

Another committee member, Sen. Jon Tester, a Democrat, said he

worried about the security of background check data, telling AP that contractors and federal agencies need to "maintain a modern, adaptable and secure IT infrastructure system that stays ahead of those who would attack our national interests."

The Office of Personnel Management and the Department of Homeland Security indefinitely halted all USIS work on background investigations in August. OPM, which paid the company $320 million for investigative and support services in 2013, later decided not to renew its background check contracts with the firm. The move prompted USIS to lay off its entire force of 2,500 investigators. A company spokesperson complained that the agency has not explained its decision. Representatives from OPM and DHS declined comment.

Last month, the federal Government Accounting Office ruled that Homeland Security should re-evaluate a $200 million support contract award to USIS. The GAO advised the department to consider shifting the contract to FCi Federal, a rival firm, prompting protests from USIS.

In the private analysis prepared for USIS by Stroz Friedberg, a digital risk management firm, managing director Bret A. Padres said the company's computers had government-approved "perimeter protection, antivirus, user authentication and intrusion-detection technologies." But Padres said his firm did not evaluate the strength of USIS' cybersecurity measures before the intrusion.

Federal officials familiar with the government inquiries said those assessments raised concerns that USIS' computer system and its managers were not primed to rapidly detect the breach quickly once hackers got inside.

The computer system was probably penetrated months before the government was notified in June, officials said. Cybersecurity experts

say attacks on corporate targets often occur up to 18 months before they are discovered and are usually detected by the government or outside security specialists.

Still, USIS noted its own security preparations "enabled us to self-detect this unlawful attack."