Personnel office not the worst in terms of lax cybersecurity

June 24 2015, byKen Dilanian

Katherine Archuleta, director, Office of Personnel Management, gestures while she testifies before the Senate Appropriations subcommittee on Financial Services and General Government hearings to review IT spending and date security at the Office of Personnel Management in Washington, Tuesday, June 23, 2015. (AP Photo/Cliff Owen)

The federal government has for years failed to take basic steps to protect its data from hackers and thieves, putting at risk everything from nuclear

secrets to the private tax information of hundreds of millions of Americans, records show.

In the latest example, the Office of Personnel Management is under fire for allowing its databases to be plundered by suspected Chinese cyberspies in what is being called one of the worst breaches in U.S. history. OPM repeatedly neglected to implement basic cybersecurity protections, its internal watchdog told Congress.

But the departments of Treasury, Transportation, State and Health and Human Services have significantly worse records, according to the most recent administration report to Congress under the Federal Information Security Management Act. Each of those agencies has been hacked in the last few years.

"Last year, across government, we the American people spent almost $80 billion on information technology, and it stinks," said Rep. Jason Chaffetz, R-Utah, chairman of the House Oversight and Government Reform Committee. "It doesn't work."

Congress can hardly escape all blame. While President Barack Obama's latest budget plan called for a $14 billion increase for cyberdefenses, the House proposed a budget in March that didn't include specific funding for cybersecurity. Nor has Congress imposed much accountability on agencies that suffer breaches.

The security lapses have persisted even as cyberattacks on government networks have increased. The federal government dealt with 67,196 cyber incidents in the last fiscal year, up from 57,971 incidents the year before, according to the White House report card, which was published in February. Missing from that document is an accounting of how many hacks were successful and what was stolen.

It's not a new problem. The Government Accountability Office has labeled federal information security a "high-risk area" since 1997. In 2003 it expanded the high-risk designation to include computer networks supporting the nation's critical infrastructure. This year, it added "personally identifiable information" to the list, just in time to see hackers steal the Social Security numbers and other private information of nearly every federal worker.

But agency managers haven't been punished for failing to secure their networks, and little sustained attention has been paid to the many intrusions.

"No one is ever held accountable," said James Lewis, a cybersecurity expert at the Center for Strategic and International Studies in Washington. Unlike in the corporate world, where the CEO of Target resigned last year after a breach of customer data, "it's been penalty free, and senior leadership doesn't really care about this."

The OPM debacle may change that. It has dealt the United States a major national security blow, experts say, by exposing the personal information, and foreign contacts, of millions of people with security clearances. OPM's director, Katherine Archuleta, told a Senate hearing on Tuesday that an "adversary" gained access to the agency's records with a credential used by a federal contractor.

Katherine Archuleta, director, Office of Personnel Management, center, talks with Michael Esser, assistant inspector general, Office of Personnel Management (OPM) Audits, left, and Richard Spires, chief executive officer, Resilient Network Systems, Inc., right, before they testify before the Senate Appropriations subcommittee on Financial Services and General Government hearings to review IT spending and date security at the OPM in Washington, Tuesday, June 23, 2015. (AP Photo/Cliff Owen)

After the OPM attack, the federal chief information officer, Tony Scott, ordered agencies to speed implementation of new security measures and fix vulnerabilities.

But many agencies seem incapable of good security practices, say industry experts, who call for a new approach that moves beyond

perimeter defenses and into sophisticated analysis of network behavior.

Scott embraces that idea. But as the government deploys new technology to discover hacks, he said in an interview, "we're going find out some things previously unknown. It's going to feel like the problem is getting worse, but it's actually getting better."

If so, evidence is thin on the ground. Last year, the Senate Homeland Security and Government Oversight Committee published a scathing report chronicling the sorry state of federal computer defenses.

"Data on the nation's weakest dams, including those which could kill Americans if they failed, were stolen by a malicious intruder. Nuclear plants' confidential cybersecurity plans have been left unprotected. Blueprints for the technology undergirding the New York Stock Exchange were exposed to hackers," the report began.

All of that was due to government lapses, the report said. In many cases, the negligence was incredibly basic. The report chronicled a failure to use sophisticated passwords, to patch software and to keep anti-virus software up to date.

While anti-virus software alone won't stop hackers from a foreign intelligence agency, the government often has also failed to take the harder steps that could deter those intruders, such as requiring a combination of smart cards and passwords for network access, and encrypting sensitive data. OPM stored Social Security numbers in unencrypted form.

Archuleta told the committee last week that many of the agency's systems were too old to support encryption, a way of putting data in code. On Wednesday, the inspector general for the OPM disputed that assertion. In written testimony, Patrick McFarland said some of the

systems involved in the data breach were modern, so encryption could have been used.

OPM's poor cyber hygiene is part of a government-wide pattern. One of the agencies that rank lowest on the annual cyber report card holds some of the most sensitive data—the Department of Health and Human Services, which keeps records on health care billing, anti-poverty benefits and child abuse.

In April, an audit found that the agency's main information technology office didn't track and manage its computer inventories effectively, failed to patch software vulnerabilities, lacked a policy to secure USB port control access, and didn't manage its anti-virus security controls effectively.

A separate audit last year found security lapses were on the rise among Medicare contractors. A third report warned of "high-risk security vulnerabilities" at 10 state Medicaid agencies.

Another potential cyber disaster area is the State Department, which had to shut down its email system this year in an attempt to clean out spyware linked to Russia. State's inspector general said in a heavily redacted report that the department is consistently failing to comply with minimum cyber standards.

The Russian spyware may be impossible to fully remove without replacing all department computers, according to a former federal law enforcement official and a private expert briefed on the situation, both of whom declined to be named because they were not authorized to discuss the matter publicly.

"We continue to find security control deficiencies in multiple information security program areas that were previously reported" each

year since 2010, the State IG report says. "Over this period, we consistently identified similar control deficiencies in more than 100 different systems."

The IRS, which holds data on Americans' income and spending habits, met federal standards in just 5 of 11 cyber security areas, the Treasury Department's inspector general latest audit concluded.

"Until the IRS takes steps ... taxpayer data will remain vulnerable to inappropriate use, modification or disclosure, possibly without being detected," the report said.

That was September. In May, the agency disclosed that hackers breached the IRS website and gained access to about 100,000 tax accounts. The intruders stole Social Security information, dates of birth and street addresses.