Written by **C. Mitchell Shaw** on June 17, 2015

Chinese Hack of U.S. Employee Database Worse Than First Reported

As we learn more about the recent cyber-attacks on U.S. federal employee records by Chinese hackers, it is becoming increasingly clear that the problem is much worse than many previously thought.

In testimony before the House Oversight and Government Reform Committee, officials within the Office of Personnel Management (OPM) admitted on Tuesday to major lapses in basic cyber-security protocols that left government systems vulnerable to at least two attacks. Those attacks allowed hackers to breach sensitive personal data about nearly all employees of the federal government and millions of persons with security clearances, according to a report by the Associated Press.

The breach was originally said to date back possibly as far as December, while new evidence suggests it lasted for more than a year. The attacks followed years of substandard security practices that made the attacks possible and prevented their discovery. As a result, both the duration and scope of the breach were far worse than they might have been had the proper protocols been in place and observed. In fact, if the proper measures had been in place, the breach could have been prevented altogether.

The attacks were also originally reported to affect only current and former federal employees and their families. Though that was disturbing enough, new reports now reveal that the breach also included information on current and former congressional staffers, raising to new levels both the numbers and intensity of the data included in the breach.

Since congressional staffers often have access to sensitive information on pending legislation, it is a frightening prospect to imagine Beijing having access to sensitive information about congressional staffers.

Even while claiming the breach did not include information on federal employees' families, officials say they are not certain exactly what data was exfiltrated. Prudence dictates a worst-case-scenario way of looking at this. Since all evidence points to Beijing, it is unreasonable to think that Chinese hackers, having access to sensitive data on millions and millions of high-ranking government employees and congressional staffers, would have hesitated for even a moment in taking the whole lot. Especially considering the time they had in which to do it and the lack of attention to security on the American side of the breach. By prioritizing the data, the hackers could have exfiltrated all of it in the time they had without drawing any attention to their activities.

OPM is basically the government equivalent to a department of human resources, keeping files on all federal employees. Those files would include the pre-employment background checks conducted on

each person — known associates, past addresses, financial information, and other data that could be used to steal the identity of (or outright impersonate) any of the employees or congressional staffers. The files would also include all employment records detailing previous positions held (in and out of government service) as well as medical records, salaries, clearances held, travel records, and other information that could be used to compromise both employees and operations.

Since all current and prospective employees seeking security clearances are required to detail the full names, Social Security numbers, dates and places of birth, and other information for spouses and partners, it is reasonable to assume that OPM is being either dishonest or naïve when it claims employees' families were not affected by the cyber-attack.

Though it is tempting to view this as the U.S. government and its employees "getting what they deserve" in the wake of the Snowden leaks, one must remember that this breach puts all Americans at risk, as China now has access to detailed information that can be collated and used to paint a very telling picture of our nation's strengths and weaknesses. As *The New American* previously reported, this data breach is indicative of China building a vast database on Americans. It is a security risk that could — and should — have been avoided.

The U.S. government should spend at least as much of its resources on protecting its own systems as it does on prying into the systems of others. Better yet, officials should cease spying on American citizens altogether and simply reallocate those resources to the protection of their own critical systems.

OPM officials had a difficult day Tuesday answering questions and receiving criticism from both Democrats and Republicans on the House Oversight and Government Reform Committee. Representative Jason Chaffetz (R-Utah), the committee's chairman, didn't soften the blow. "You failed utterly and totally," he told the OPM officials present at the hearing.

The testimony offered by Michael Esser, OPM's assistant inspector general for audit, was condemning of the ineptitude (or worse) present in the agency. He testified that he had warned of severe shortcomings including OPM's lack of meeting federal cyber-securty standards, and unqualified information technology personnel being in charge of system security. The audit conducted by Esser's office recommended in November that the OPM pull the plug on some networks due to security risks associated with those shortcomings.

Even that may have been too little too late, since it is now known that the breach was months old by that point. Chairman Chaffetz told OPM Director Katherine Archuleta that not following the recommendation of the audit was unacceptable. "They recommended it was so bad that you shut it down and you didn't," he charged. Archuleta attempted to defend her decision by claiming that shutting down those networks would have hindered OPM's mission. One wonders if OPM's mission is to provide an easy back door for Chinese hackers to steal sensitive data on government employees. Otherwise, why not simply comply with industry standards for securing the data?

The committee called for Archuleta's apology and resignation. Keeping with her trend, she did not follow that recommendation either. Instead, she led the committee in a rousing round of pin-the-blame-on-the-system. "The whole of government is responsible and it will take all of us to solve the issue," she insisted.

In the free market that drives the economy of this nation, the result of this degree of failure to perform the basic functions of one's job would certainly end in dismissal. It is obvious that officials at this government agency are either inept or worse. Concerned Americans should demand a complete

housecleaning at OPM.