Republican Perspective
24 June 2015
by Ed Manning

CAN LIFE-LOCK HELP OBAMA?

"It has become appallingly obvious that out technology has exceeded our humanity." Albert Einstein

The U.S. may be facing a different type of war and may already be under attack by a foreign sovereign government. We learned that the Federal Office of Personnel Management (OPM) suffered a cybersecurity attack where 4.2 million records of current and retired federal workers were stolen. Security experts said the attack had the markings that it came from China.

The OPM concluded "with a high degree of confidence" that the agency's computer system's containing information related to the background investigations of "current, former and prospective" federal employees were breached. Information on officials as senior as Cabinet secretaries may have been compromised. Perhaps President Obama should require all federal agencies to buy the identity theft software "Life-Lock"?

The personal information data breach of the OPM is the mother lode for countries considered our adversary. The information compromised included financial histories and investments, children's and relatives names, past residences and the names of neighbors and close friends.

U.S. Intelligence agencies have been hiring more people of Asian and Middle Eastern descent, some of whom have relatives living overseas. The fear is that our adversaries will use leverage over Americans that have access and knowledge of the country's intelligence secrets by pressuring their overseas relatives. The Obama administration was forced to announce that a second attack occurred where hackers obtained background information on millions of military, intelligence personnel and other individuals who have been investigated for security clearances. The feds now say that nearly 14 million records were stolen.

What is disturbing is that the OPM breach may have been prevented if it had followed the federal rules for information security. The Federal Information Security Management Act outlines steps an agency must take to secure its systems. In 2014, the inspector general for OPM found many areas where it did not follow these baseline security practices. It's not so much the technical prowess of the Chinese but the lackadaisical approach of the Obama administration to securing government computer systems.

Michael Esser, an assistant inspector general with the OPM, testified before the House oversight committee that many of the people hired to run the agency's Information

Technology department had no computer experience, and that the agency itself did not discipline its employees after it failed several security audits. This should not be surprising as there is little accountability of federal employees. Look no further than former Secretary of State Hillary Clinton's use of a private email account while conducting government business.

It will only be a matter of time that we hear from the Left, that more of our money is needed to fix the security problem. The feds are spending $10 billion a year to protect sensitive data but can't stay ahead of sophisticated hackers. Is it any wonder when the nation's human resources agency hires people with no computer skills to work in its IT department. If this wasn't such a serious matter it would make for good comedy.

Cyber attacks have been occurring with increasing frequency. In 2013, security officials responded to a total of 228,700 cyber incidents involving federal agencies and contractors.
Federal employees continue to ignore basic security protocols that adds to the problem according to government security experts.

In June of 2014, USIS, the government's leading security clearance contractor, reported that a cyberattack had compromised the records of at least 25,000 Homeland Security employees. In October of 2014, Senate investigators reported that China's military hacked into computer networks of civilian transportation companies hired by the Pentagon at leasts nine times. They also hacked into computers on a commercial ship, targeted logistic companies and uploaded malicious software onto an airline's computer.

The FBI did arrest a National Weather Service employee, Xiafen Chen, for illegally downloading restricted files from the National Inventory of Dams which contain sensitive information about vulnerabilities in the nation's 85,000 dams.

Federal intelligent officials now state that cybersecurity is the number one threat facing the U.S.
They obviously didn't hear the President's statement that "no challenge poses a greater threat to future generations than climate change." The main stream media should cease being a lapdog and report the seriousness of these cybersecurity attacks and the impact to both our intelligence apparatus and military with its mission to protect the nation. Little will come from the White House…

Note: Republicans please visit our newly revised website: www.rossmoor-republican.us. You can stay current on candidates and fund raisers as well as other issues.