Written by **C. Mitchell Shaw** on November 21, 2015

Inspector General: DHS Risks National Security

The Department of Homeland Security is risking national security by illegally maintaining 136 "sensitive but unclassified," "Secret," and "Top Secret" systems with "expired authorities to operate", according to an audit released Thursday by the office of the inspector general. Because these databases do not have current "authorities to operate (ATOs)", DHS "cannot ensure that its systems are properly secured to protect sensitive information stored and processed in them," the inspector general said. Maybe the department should change its name to the Department of Homeland Insecurity.

The release of the audit confirms and underscores what many have long suspected: by creating databases which house information on the communications, activities, relationships, browsing histories, and other personal information of American citizens and businesses, government agencies create a security risk where there is a single point for hackers — private and government — to focus. As this writer said about China's hacking of the databases at the Office of Personnel Management (OPM):

> It's a little like the trick-or-treating strategy employed by street bullies: Rather than do the hard work of going door-to-door collecting the loot, let someone else do it for you and then simply steal it from them. With U.S. government three-letter agencies conducting intrusive surveillance on the American people, the shortest path to that data is to hack those databases and steal it. And it appears this is exactly what China is doing. This is precisely what groups such as the Electronic Frontier Foundation have warned about as part of their opposition to the blanket surveillance conducted by these overreaching agencies.

Besides China's attack on the systems at OPM, Russian hackers breached systems at the White House and in a separate attack inserted a destructive "Trojan Horse" into computer systems vital to national security (besides being responsible for the massive hack at Sony that nearly destroyed the company and for which North Korea was made the scapegoat). It should therefore require no imagination at all to envision sensitive information about nearly all American citizens falling into the hands of foreign powers hostile to this nation. Adding to the evidence of government ineptitude and incompetence is the fact that the White House had to be informed by a foreign ally that its systems had been hacked. As we reported then:

> One of the most disturbing elements in this case is that the hacking was not even discovered by the White House. The *Washington Post* reports that an "ally" made U.S. officials aware of it. There was no information on who the ally was or how it knew of the hacking. It is ironic that the U.S. government was oblivious to a hacker breaking into its computers considering how intent it is in breaking into the computers of others.

By maintaining these sensitive databases and systems without ATOs (Authorities To Operate), DHS has demonstrated that its goals in conducting the blanket surveillance — for which this and other publications have criticized it — have less to do with securing national security and more to do with spying on American citizens for its own purposes. If the goal was national security, the agency would have operated both within the law and within proper security protocols. It has done neither.

As the *Washington Free Beacon* reported:

> The audit also found that security patches were missing for computers, Internet browsers, and databases, and weak passwords left the agency's information security vulnerable.
> "We found additional vulnerabilities regarding Adobe Acrobat, Adobe Reader, and Oracle Java software on the Windows 7 workstations," the inspector general said. "If exploited, these vulnerabilities could allow unauthorized access to DHS data."
>
> The review, which was mandated by the Federal Information Security Modernization Act of 2014, found that internal websites were also susceptible to "clickjacking" attacks and "cross-site and cross-frame vulnerabilities."
>
> "Cross-site and cross-frame scripting vulnerabilities allow attackers to inject malicious code into otherwise benign websites," the inspector general said. "A clickjacking attack deceives a victim into interacting with specific elements of a target website without user knowledge, executing privileged functionality on the victim's behalf."

According to the audit, the office of inspector general "made six recommendations to the Chief Information Security Officer." Of those six, the audit says, "The Department concurred with five recommendations." The decision by DHS to "concur" on five of the six recommendations is not very comforting. In truth, the department has proved itself to be unworthy of the degree of trust government officials have shown it. These security risks never should have existed in the first place.

Furthermore, considering the attacks on government and industry systems by both foreign powers and hacker groups over just the last year, it is inexcusable that DHS had to get caught with its pants down before "concurring" that it needs to be more careful. DHS officials seem not to have learned anything from the past, and it would be foolhardy to trust that they have learned anything from this.

The timing of the release of this audit is noteworthy as it comes on the heels of calls for more surveillance and an end to private citizens' use of encrypted communications following the deadly attacks on Paris last week. In light of the findings of this audit, it would seem that rather than increasing surveillance and weakening the privacy of citizens, the proper response would be exactly the opposite.

It would also seem wise to consider disassembling the apparatus and agencies that have not only threatened the privacy and liberty of Americans, but can now — more than ever — be shown to have threatened the security Americans were promised in exchange for that lost privacy and liberty.