Published on ***ISE.gov*** (http://ise.gov)

Senators Lieberman and Collins: How to Prevent the Next WikiLeaks Dump

Posted by Anonymouson Wednesday, January 26, 2011

- Subscribe [1] [2]

Wednesday, January 26, 2011

How to Prevent the Next WikiLeaks Dump

The solution isn't to go back to the pre-9/11 era, when agencies hoarded information

By JOSEPH I. LIEBERMAN AND SUSAN M. COLLINS

When a U.S. Army intelligence analyst stole some 260,000 classified State Department diplomatic cables and gave them to WikiLeaks last year, he set off a digital-age collision. He also launched a debate about how to balance the values of a free and open society with our legitimate security needs.

We all support transparency, but these criminal leaks were not about open government. WikiLeaks's recklessness compromised our national security and could put the lives of our citizens, soldiers and allies at risk. Any claim that they were stolen and published on the Web in the name of "transparency" or "accountability" is belied by a cable WikiLeaks released that identifies sites around the world critical to U.S. national security, such as undersea communications cables, vaccine makers, and manufacturers of weapons parts. There is no justifiable reason for releasing this document: The intent can only have been to damage the United States and our allies.

Facilitating better information-sharing among federal law enforcement and civilian and military intelligence agencies was an important part of legislation enacted after the attacks of 9/11, including the Intelligence Reform and Terrorism Prevention Act of 2004, which we authored. Starting in 2006, the State Department made its cables available to military and intelligence agencies with the hope that the information could be used to detect and break up terrorist plots before they occurred.

The problem is that this information-sharing also made it possible for Army Pvt. Bradley Manning to access these cables?most of which had nothing to do with his intelligence duties in Iraq.

Clearly, we need to improve our network security. But a return to the pre-9/11 era, when agencies hoarded information, would compromise our national security. The 9/11 Commission found 10 specific incidences in which, had our law enforcement and intelligence agencies shared information, the attacks might have been prevented. Since the 9/11 Commission reforms have been implemented, we know that several major terrorist plots have been thwarted because federal intelligence and law enforcement agencies have successfully shared information with state and local law enforcement, as well as with our overseas allies.

The military's recent decision to completely ban the use of external storage devices like memory sticks and compact discs on sensitive computers is an appropriate temporary solution. But we must ensure that this measure doesn't hinder vital information-sharing in battlefield or crisis conditions.

All manner of technological and management controls should be explored to reduce the risk of unauthorized disclosures while enabling critical analysis of intelligence and other data. For instance, the 9/11 Commission Recommendations Act of 2007 required that military and civilian intelligence information-sharing systems install audit capabilities that would alert supervisors to suspicious download activity. Had this kind of security measure been in place, security officers might have detected the analyst's massive downloads before he was able to pass the cables on to WikiLeaks.

Relevant federal government agencies need to move quickly to develop and install these sorts of measures that are already working elsewhere in the intelligence community.

Another important step would be to move to "role-based" access to secure information. Instead of making all information available to everyone who has access to classified systems, a role-based system makes information available based on individuals' positions and the topics for which they are responsible. For example, State Department cables from a given embassy would be available to military officials who are deployed in that country or who work on issues related to that country, but not to the full population of cleared Department of Defense employees.

In sum, we must craft security solutions that balance the imperative to share sensitive information with the need to prevent disclosures that are harmful to national security.

Mr. Lieberman is an Independent Democratic senator from Connecticut. Ms. Collins is a Republican senator from Maine.

Source URL: http://ise.gov/news/senators-lieberman-and-collins-how-prevent-next-wikileaks-dump

Links:
[1] http://ise.gov/ise-news/feed
[2] http://public.govdelivery.com/accounts/USODNIISE/subscriber/new?topic_id=USODNIISE_29