Information Security and Fear-Mongering about WikiLeaks

The response of the White House’s Office of Management and Budget (OMB) to a recent WikiLeaks document dump gives us a peek both into the sometimes surreal standards for dealing with information that the executive branch deems to be classified and at the fear-mongering in which some government officials are engaging.

According to CNN, on December 3, OMB instructed executive branch agencies to notify all government employees and contractors that they should not view any documents that are marked as classified using their work computers that access the web via nonclassified government systems.

OMB distinguished “documents that are marked classified” from “news reports … that … discuss the classified material.” Apparently, employees are permitted to use nonclassified government systems to access news reports that include classified information, but must not use those systems to access the classified documents themselves.

This distinction might seem silly to an outsider, but the government imposes special security measures for its computers that store classified documents, and takes pains to ensure that its computers without those security measures do not have any classified documents. This system of segregating classified documents is complicated and costly. But so far, so good.

OMB also suggested (somewhat ambiguously) that federal employees and contractors without the proper clearances and the “need to know” the information should not access WikiLeaks’ classified information.

Additionally, at least one agency went further, asserting that government employees—and prospective employees—should not access WikiLeaks classified documents even from their home computers. According to Democracy Now, the State Department instructed employees of the U.S. Agency for International Development as follows: “Accessing the WikiLeaks website from any computer may be viewed as a violation of the SF 312 agreement.”

Indeed, according to the SF 312 (a nondisclosure agreement), violation can result in termination of a security clearance and employment. The State Department memo also warned USAID employees: “Any discussions concerning the legitimacy of any documents or whether or not they are classified must be conducted within controlled access areas (overseas) or within restricted areas (USAID/Washington) … The documents should not be viewed, downloaded, or stored on … a USAID unclassified network computer or home computer; they should not be printed or retransmitted in any fashion.” In other words, just accessing the WikiLeaks website from a home computer could result in the loss of a security clearance and job.

Steven Aftergood, director of the Federation of American Scientists Project on Government Secrecy—a transparency activist who has been critical of WikiLeaks—rightly characterized the State Department memo as “insane.”

It is not at all clear how accessing the WikiLeaks documents on a personal home computer would constitute a violation of an agreement not to disclose classified information. On the other hand, the SF 312 asserts that “unauthorized retention … of classified information … could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation.”

This does not appear to be a one-off mistake by an overzealous State Department official as at least one government contractor similarly warned its employees against accessing WikiLeaks both on company-issued and on personal equipment. Indeed, Career Services offices at Columbia University and Boston University also reportedly warned students and alumni about the risks of posting links to the documents and/or commenting on them through social media.

Are these just over-reactions by people who are not familiar with the government’s information security standards? Or do these warnings reflect a concerted effort to prevent Americans from accessing and discussing the WikiLeaks documents that are now available on the web? I sincerely hope that someone in government will provide some clarification—and some sanity—on this issue soon.

Kathleen Clark, professor of law and the 2010–11 Israel Treiman Faculty Fellow, teaches and writes about government ethics, national security law, legal ethics, and whistleblowing.