United States Department of the Interior

U.S. GEOLOGICAL SURVEY
Reston, Virginia 20192

In Reply Refer To:
Mail Stop 205

Dear Sir or Madam:

On December 6, 2010, the attached memorandum entitled "Safeguarding of Classified Information and Use of Government Information Technology Systems" was issued by the Department of the Interior, Office of the Solicitor. The U.S. Geological Survey (USGS), Office of Acquisition and Grants, is disseminating this memorandum to all USGS contractors and financial assistance recipients as "each federal employee and contractor is obligated to protect classified information pursuant to all applicable laws, and to use government information technology systems in accordance with agency procedures so that the integrity of such systems is not compromised."

Please contact your cognizant Contracting Officer or Grants Officer if you have any questions in regards to the attached memorandum.

Sincerely,

/s/
Scott G. Morton
Chief, Office of Acquisition and Grants

United States Department of the Interior

OFFICE OF THE SOLICITOR
Washington, D.C. 20240

IN REPLY REFER TO:

DEC - 6 2010

Memorandum

To: All DOI Employees and Contractors

From: Solicitor

Subject: Safeguarding of Classified Information and Use of Government Information Technology Systems

The recent disclosure of U.S. Government documents by WikiLeaks has resulted in damage to our national security. Each federal employee and contractor is obligated to protect classified information pursuant to all applicable laws, and to use government information technology systems in accordance with agency procedures so that the integrity of such systems is not compromised.

Unauthorized disclosures of classified documents (whether in print, on a blog, or on websites) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, ***classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by federal employees and contractors, until it is declassified by an appropriate U.S. Government authority.***[1] Although the Department has blocked access to the WikiLeaks web site from Departmental computers, it is important to understand our continuing duties and responsibilities in this regard.

Federal employees and contractors therefore are reminded of the following obligations with respect to the treatment of classified information and the use of non-classified government information technology systems:

- Except as authorized by their agencies and pursuant to agency procedures, federal employees or contractors shall not, while using computers or other devices (such as Blackberries or Smart Phones) that access the web on non-classified government systems, access documents that are marked classified (including classified documents publicly available on the WikiLeaks and other websites), as doing so risks that material still classified will be placed onto non-classified systems. This requirement applies to access that occurs either through agency or contractor computers, or through employees' or contractors' personally owned computers that access non-classified government systems. This requirement does not restrict employee or contractor access to non-classified,

[1] Executive Order 13526, *Classified National Security Information* (December 29, 2009), Section 1.1.(c) states, "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information."

publicly available news reports (and other non-classified material) that may in turn discuss classified material, as distinguished from access to underlying documents that themselves are marked classified (including if the underlying classified documents are available on public websites or otherwise in the public domain).

- Federal employees or contractors shall not access classified material unless a favorable determination of the person's eligibility for access has been made by an agency head or the agency head's designee, the person has signed and approved non-disclosure agreement, the person has a need to know the information, and the person has received contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

- Classified information shall not be removed from official premises or disclosed without proper authorization.

- Federal employees and contractors who believe they may have inadvertently accessed or downloaded classified or sensitive information on computers that access the web via non-classified government systems, or without prior authorization, should contact their information security offices for assistance.

Thank you for your cooperation, and for your vigilance to these responsibilities. If you have any questions regarding handling classified documents, please contact Mr. Christopher Riemer in the Office of Law Enforcement, Security and Emergency Management at (202) 208-6206. If you have questions regarding the blocking of access to the WikiLeaks web site, please contact the Chief Information Security Officer (CISO) for your bureau or office. The current list of bureau and office CISOs and their contact information is available at https://portal.doi.net/CIO/CSD/BUREAUS/default.aspx.