5-19-16

U.S. Department of Justice

Justice Management Division

Office of General Counsel

Washington, D.C. 20530

MAY 12 2016

The Justice Management Division (JMD) received a referral from the Office of Information Policy (OIP) of a two-page memorandum responsive to your Freedom of Information Act (FOIA) request seeking senior management office memoranda posted on DOJNET. As the document originated in JMD, OIP referred it to JMD for a determination as to release and for direct response to you. We have reviewed the memorandum and have determined that it may be released. The document is enclosed.

Sincerely,

Arthur E. Gary
General Counsel

cc: James Davis (OIP)

MEMORANDUM FOR JMD EMPLOYEES AND CONTRACTORS

FROM: Lee J. Lofthus
Assistant Attorney General
for Administration

SUBJECT: WikiLeaks - Safeguarding Classified Information and Use of Government Information Technology Systems

The recent disclosure of U.S. Government documents by WikiLeaks has resulted in significant damage to our national security and raised questions about safeguarding classified information and using unclassified Government IT systems to access this information.

All DOJ employees and contractors are reminded of the following obligations with respect to the treatment of classified information:

- DOJ employees and contractors are individually obligated to protect classified information pursuant to all applicable laws and to use government information systems appropriately.
- Unauthorized disclosures of classified documents (whether in print, on a blog, or on a website) 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 (Executive Order 13526, Section 1.1.(c)).

All DOJ employees and contractors have the following obligations with respect to the use of non-classified government information technology systems:

- DOJ employees or contractors shall not access information marked or labeled as classified (including material publicly available on the WikiLeaks website or other websites) using non-classified government computers or other government

devices that access the web (such as Blackberries or Smart Phones), as doing so risks placing material that is still classified on non-classified systems. This restriction does not limit employee or contractor access to non-classified, publicly available news reports (and other non-classified material) that in turn reference classified material, as opposed to the underlying classified material itself (whether or not in the public domain).

- DOJ employees or contractors who believe they may have downloaded classified information to a non-classified government system should contact the JCON help desk (6-7100) for assistance.

If an individual has a legitimate need to access classified information on publicly available websites, the individual shall work through the Department Chief Information Officer to ensure such access in managed in a manner that minimizes risk to DOJ information systems.

Questions regarding the Department's IT security program may be directed to Kevin Deeley, Chief Information Security Officer, (Kevin.Deeley@usdoj.gov, 202-353-2421). Questions regarding other Department security programs may be directed to Glenn Bensley, Assistant Director, Security and Emergency Planning Staff (Glenn.R.Bensley@usdoj.gov, 202-514-4798).