# NOTICE
# TO CONTRACTORS CLEARED UNDER THE NATIONAL INDUSTRIAL SECURITY PROGRAM
# ON
# PROTECTING CLASSIFIED INFORMATION AND THE INTEGRITY OF GOVERNMENT DATA ON CLEARED CONTRACTOR INFORMATION TECHNOLOGY (IT) SYSTEMS

Defense Security Service
February 11, 2011

The recent disclosure of U.S. Government documents by WikiLeaks has caused damage to our national security. On January 11, 2011, the Acting Undersecretary of Defense (Intelligence) directed the Defense Security Service (DSS) to notify cleared companies of their obligations to protect classified information and to follow established and authorized procedures for accessing classified information. This direction was accompanied by a notice applicable to Department of Defense employees. DSS previously issued a reminder to cleared contractors on December 13, 2010 regarding accessing publically posted classified information.

This notice reiterates basic existing obligations and principles governing the protection of classified information for contractors cleared under the National Industrial Security Program (NISP). Contractors are obliged to ensure that their cleared employees and consultants protect classified information and the integrity of US government data within IT systems in accordance with applicable laws, national and DoD policies, contracts and agreements. Contractor employees at government installations are reminded that they are to follow the security requirements of the host installation.

Unauthorized disclosures of classified documents (whether in print, on a blog, or on websites) does not alter the document's' 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, until it is declassified by an appropriate original classification authority.***

Cleared contractors should remind their employees of the following obligations with respect to protecting classified information:

- Cleared contractor employees shall not access classified information unless they have:
    - received a determination, by an appropriate authority, that they are eligible for access to classified information,
    - signed an approved nondisclosure agreement,
    - demonstrated a need to know the information, and
    - received 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.

- Cleared contractor employees shall not remove classified information from official (government or company) premises or disclose it without proper authorization.

- Except as authorized by U.S. Government policy and procedures, cleared contractor employees shall not, while accessing the web on unclassified systems (i.e., systems not certified and accredited to process classified information, including BlackBerries or other smartphones), access or download documents that are marked as classified (including classified documents publicly available on Wikileaks.org or other websites), as doing so risks putting classified information on unclassified IT systems. Such downloading or accessing of classified information may constitute a security violation and shall be processed as such by the cleared contractor and DSS.

- This requirement applies to accessing or downloading classified information that occurs using company-owned unclassified computers or employees' personally owned computers that access unclassified government systems, either through remote Outlook access or other remote access capabilities that enable connection to government systems.

- This does not restrict access to unclassified, publicly available news reports (and other unclassified material) that may discuss classified material, as distinguished from access to the underlying classified documents available on public websites or otherwise in the public domain.

- Cleared contractors should neither confirm nor deny the presence of classified information in articles or websites in the public domain. Doing so may constitute a security violation.

- Cleared contractor employees who believe they have **inadvertently** accessed or downloaded classified information from a public website via an unclassified IT system, or without prior authorization, shall contact their information systems security officer (ISSO), information systems security manager (ISSM) and Facility Security Officer (FSO) for assistance.

The widespread distribution of the documents posted on WikiLeaks has prompted the requirement to use other than normal spill procedures, as identified below. Due to the extent of the compromise and the prohibitive cost of standard sanitization procedures for this information, the following guidance is provided for responding when classified documents have been inadvertently accessed or downloaded from the WikiLeaks website or other websites posting WikiLeaks-released classified documents:

- *For Windows-based systems, the lSSO / ISSM will document each occurrence and delete the affected file(s) by holding down the SHIFT key while pressing the DELETE key.*
- *For other than Windows-based systems, a similar "delete" technique shall be used for the affected file(s).*
- *No incident report or further sanitization of IT systems is required. However, documentation concerning the occurrences should be forwarded to DSS ODAA for data collection purposes.*

Thank you for your cooperation and vigilance in implementing these responsibilities.

Questions should be addressed to your Industrial Security Representative.