209 596

THE UNDER SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

380.015

April 7, 2011

MEMORANDUM FOR SECRETARY OF DEFENSE

SUBJECT: Army Review of the Compromise of Classified Information to Wikileaks

In response to your memorandum dated March 3, 2011, the Department of the Navy has completed a review of all pertinent regulations, policies, and training programs associated with the handling and safeguarding of classified National Security Information (NSI). A summary of this review is contained in Attachment 1.

In addition to the identified areas of concern noted in the attachment, the Wikileaks event created a situation wherein the Department of Defense and the Department of the Navy must consider how classified NSI should be treated in the event the information migrates to, or is viewed from, a DON unclassified network. To that end, revised procedures have been promulgated DON-wide for reporting, handling and responding to this type of event. Additionally, there were several areas identified in which the DON could improve regarding the handling of classified NSI within the .mil domain to include the processing, storing, transmission and proper marking of classified information. The DON is taking actions to improve in these areas.

Should your staff require further assistance in this matter, my point of contact is (b)(6) who may be reached at (b)(6).

Robert O. Work

Attachment:
As stated

7 APR 11

OSD 04119-11
4/8/2011 10:39:39 AM

DEPARTMENT OF THE NAVY

CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

ACTION MEMO

31 March 2011

FOR: SECRETARY OF NAVY

UNSECNAV 4/7

FROM: (b)(6) (b)(6), Department of the Navy Chief Information Officer

SUBJECT: Army Review of the Compromise of Classified Information to Wikileaks

- TAB A is proposed Department of the Navy response pursuant to direction contained in TAB B.

- Issuance of TAB A will satisfy the requirement tasked in the Secretary of Defense's memorandum of March 3, 2011 (TAB B) which directs the Military Departments to review pertinent regulations, policies, and training programs to address any systematic shortfalls in several areas, including information security, physical security and information assurance. Results are to be reported to the Secretary of Defense by April 4, 2011.

RECOMMENDATION: SECNAV sign TAB A.

COORDINATION: See TAB C

ATTACHMENTS:
As stated

Prepared by: (b)(6), DON CIO, (b)(6)

REVIEW OF INFORMATION ASSURANCE, INFORMATION AND PERSONNEL SECURITY PROGRAMS

Area of concern: Only Service members meeting prescribed standards of fitness (both physical and mental) reliability, and trustworthiness are deployed to a theater of operations.

Finding: Within the Department of the Navy (DON), we provide directive guidance for the screening of service members to ensure prescribed standards of fitness, reliability, and trustworthiness are met prior to deployment to a theater of operations.

The Chief of Naval Operations (OPNAV) Instruction 1300.14D provides for screening as follows:

- The overseas screening policy screens all orders to a home port or permanent duty station in CONUS and remote duty in OCONUS.
- The operational screening policy screens all Sailors going to a CONUS operational command that may deploy in a theater of operations.
- The Individual Augmentation (IA) screening is designed to properly screen all Sailors ordered to an Overseas Contingency Operation (OCO).

The Marine Corps program provides for screening of personnel as follows:

- Marine Corps Order (MCO) P1300.8R (Marine Corps Personnel Assignment Policy) requires screening of Marines prior to overseas/operational assignment.
- MCO P1326.6D (Selecting, Screening, and Preparing Enlisted Marines for Special Duty Assignments and Independent Duties) issues additional screening criteria for specialized assignments (security forces, independent duty etc.).

In all cases, the Commanding Officer is expected to withhold orders if the member fails any portion of the screening, regardless of circumstance.

Attachment 1

Area of concern: Personnel assigned to duties with responsibilities for information, or personnel security, or information assurance, at any level, are properly appointed, trained, and prepared to execute those responsibilities.

Finding: Within the DON, we provide policy for appointing Special Security Officer (SSO), Personnel Security, Information Security and Information Assurance personnel in writing. There are training programs associated with each level of responsibility; however, challenges exist for acquiring and/or maintaining training and certifications:

- Information/Personnel Security: Formal schoolhouse training for the DON Command Security Managers (CSM) course is not adequately resourced to accommodate all CSMs appointed. Those unable to attend formal schoolhouse training may receive training through the Defense Security Service Academy, applicable correspondence courses, or Computer Based Training (CBT) at no cost to the service member. Compliance is enforced utilizing the Inspector General inspection process. Additionally, USMC is piloting an information and personnel security program tool, which will have tracking and oversight capability.

- Information Assurance: Although initial formal schoolhouse training remains funded for FY12 and beyond, funding for IA certification training, testing, and maintenance along with Operating System (OS) and Computing Environment (CE) training and certification is currently an unfunded requirement. Improving the DON's ability to provide continuing education and training/certification outside of formal schoolhouse training is at severe risk. Will address in POM 13.

- Special Security Officer (SSO): As there is no formal DON standardized schoolhouse training for the SSO, the Sensitive Compartmented Information (SCI) training of SCI security professionals on the SCI program management and SSO responsibilities relies heavily on Navy SSO-sponsored policy seminars, Computer Based Training (CBT) products and Navy Knowledge Online (NKO). Residence and mobile SSO training through the Defense Intelligence Agency (DIA) and Office of Director of National Intelligence (ODNI) is also available. DON funding for SSO CBT development is approximately $100K - $150K annually. Training development in the last five years has been funded utilizing SSO Navy's operational funds because there is no current funding line dedicated to SCI program training initiatives. This issue will be addressed in POM-13. High priority training will be adjusted in FY12.

Area of concern: Adequate guidance is in place to address knowledge management and information assurance requirements for tactical units.

Finding:

Knowledge Management (KM):

- Top level DON guidance is in place to address both shore based/garrison units and forward deployed tactical units. Specific to the tactical level, direction is provided by Operational Task Orders (OPTASK) for Information Management (IM) and/or Knowledge Management (KM). All Carrier Strike Groups (CSG) and Amphibious Readiness Groups (ARG) maintain current OPTASK IM/KM as well as a separate OPTASK Chat.

- Tactical level IM and KM execution is supported by commands that assess, assist, and train CSGs and ARGs. The standards on which these evaluations are based are Navy Mission Essential Task Lists (NMETLs). As the name implies, these lists delineate the many tasks at which a CSG or ARG must excel to effectively lead their groups. The Commander, Fleet Cyber Command approved NMETLs include 23 measureable tasks for IM and KM.

- Commander Strike Force Training Pacific (CSFTP), Commander Strike Force Training Atlantic (CSFTL), Tactical Training Group Pacific (TTGP) and Tactical Training Group Atlantic (TTGL) all participate in the execution of Fleet Response Training Plans (FRTPs) for every CSG and ARG prior to deployment. FRTPs include instruction, mentoring, command evaluations, CSG and ARG "school house" training events, simulated shipboard exercises, war-gaming and training exercises at sea. IM and KM are important and graded portions of these evolutions. Both the simulated shipboard and at sea training are based on NMETs. In addition, the Marine Corps captures knowledge and experiences regarding systems and Tactics, Techniques and Procedures to remedy deficiencies and reinforce successes.

- Training: There is a strong training component to the execution of FRTPs described above. Additionally, classroom KM training is provided in the semi-annual TTGP Afloat Knowledge Managers Course; training for DON personnel is offered by the DON Chief Information Officer Command KM course. In addition, the Naval Postgraduate School provides KM/IM degree and certificate programs.

Information Assurance:

- SECNAV Instruction 5239.3B, DON Information Assurance Policy, assigns responsibilities in the DON for developing, implementing, managing, and evaluating DON Information Assurance (IA) programs, policies, procedures, and controls. The instruction is applicable to tactical units. Both Navy and Marine Corps have promulgated Service level IA policies to further amplify the DON policy. In addition, the Marine Corps has 15 enterprise IA directives covering specific implementations of cybersecurity policy.

- Annual DON IA training, as well as additional training, is provided to support job specific requirements of the IA workforce as required by the DoD 8570 series.

- Oversight is provided through the Naval Audit Service and Inspector General.

Area of concern: State of the art information assurance and network security tools are deployed on Naval information systems and network.

Finding:

- United States Cyber Command (USCC) directs implementation of security capabilities on DoD networks. In response to USCC direction in December 2010, the DON accelerated deployment of Host Based Security System (HBSS) with Device Control Module (DCM) on afloat SIPR systems from 4QTR FY14 (programmed) to 4QTR FY11. DCM provides the capability to centrally control a user's ability to copy or move files to removable media. Installations began in February 2011 and will continue through September. All afloat units, including Military Sealift Command, will have HBSS installed on their SIPR systems. HBSS installation on ashore SIPR will be completed by mid-May 2011.

- DON networks deploy a variety of security tools such as firewalls, intrusion detection sensors, anti-virus, anti-spy ware, spam filtering agents, host based intrusion prevention systems, vulnerability scanning tools, vulnerability remediation tools, and network boundary sensors to create defense in depth on Naval networks.

- Marine Corps HBSS deployment is already above 93 percent. In addition to HBSS, Marine Corps network security tools include anti-virus and intrusion detection and protection systems in both garrison and tactically deployed networks. Portion of the DON use the current Department of Defense (DoD) standard vulnerability scanning and remediation tools, eEye Retina and Hercules. EnCase is used for forensic analysis.

- The Marine Corps is also piloting the use of potential continuous monitoring and remediation tools, specifically a combination of Symantec Altiris, BigFix, and Palo Alto protocol firewalls. Initial indications show a patch remediation capability that ensures a 97 percent compliance rate. The DON has implemented cryptographic log-on (CLO) tools, using the Common Access Card (CAC) as the identification and authentication token. Portions of the DON have implemented CLO in both garrison and tactical environments. The Marine Corps also conducts monthly service-wide scanning from the Marine Corps Network Operations and Security Center (MCNOSC), supplemented by regional scanning conducted by the regional Blue Teams using eEye Retina and a DoD wireless assessment tool, Flying Squirrel.

- The DON enforces an annual all-hands requirement for completion of IA training as well as specialized training/certifications for personnel involved with operation of security tools. Similarly, all hands with a security clearance are required to receive annual physical security and counter-intelligence refresher training, and supervisors are reminded to monitor their personnel for any indications of failure to comply with proper classified material handling procedures (verbal, written, or electronic).

- Resourcing for IA workforce training (initial, retraining, and maintenance) is inadequate to keep pace with the increase in IA activities and technology. In addition, the Services cannot successfully defend cybersecurity/IA budget lines intended as placeholders to allow compliance with emergent execution year requirements from USCC. This issue will be reviewed in POM-13.

Area of concern: Service policy for the control of re-writeable media is adequate and enforced.

Finding:

- Commanding Officers and Officers in Charge are responsible for ensuring that removable storage media (floppy disk, compact disc, USB) use complies with SECNAV Instruction M-5510.36 (DON Information Security Program). This guidance remains in effect for all rewritable media other than flash media.

- U.S. Strategic Command (USSTRATCOM) 142359Z NOV 08 prohibiting use of flash media remains in force. In addition, USCC 122335Z FEB 10 CTO 10-04 provides specific guidance on use of flash media on DoD networks and NETWARCOM NTD 04-07 provides Navy-specific guidance on use of flash media. Commanding Officers and Officers in Charge are responsible for implementation and control of flash media use on and with DON networks.

- USCC CTO 10-133, NETWARCOM CTO 10-25A, and Marine Corps Administrative Message (MARADMIN) 025/11 limit write capability on SIPRNET. Navy second echelon commands have been directed to institute internal management controls, maintain logs of SIPRNET file transfers to removable media, and conduct periodic inspections of activities at subordinate commands. Additional inspection at the individual command level is being incorporated into NETWARCOM Cyber Security Inspections Program as part of operational compliance for the Navy and as part of the Marine Corps Inspector General program. A Marine Corps report names individuals specifically authorized write-privileges on the SIPRNET, and at present this is limited to only 493 individuals across the Marine Corps.

- Technical solutions for restricting writing to removable media are expensive, difficult to sustain and have the potential for operational impact. Commands must enforce existing policies regarding the proper handling of classified material, conduct regular training, to include Plan of the Day/Week notes, and hold our personnel accountable for their actions.

Area of concern: Service policy with regard to entry and exit inspections in Sensitive Compartmented Information Facilities and other secure areas is adequate and enforced.

Finding:

- DON SCI policy directs Senior Intelligence Officers (or equivalent) to ensure a continuing security program for periodic unannounced and random inspections of all hand carried articles brought into or removed from the Sensitive Compartmented Information Facility (SCIF). The primary responsibility for the entry/exit inspections rests with the SSO/Contracting Special Security Officer (CSSO) (or their designee) in coordination with the IA Manager.

- Entry/exit inspections may occur at anytime, with emphasis placed on the beginning and end of the duty day. A record of entry/exit inspection is maintained, reflecting the date and time the inspection occurred and any incidents noted. Frequency and number of inspections is established by the Senior Intelligence Officer.

- The Naval Intelligence Community Security Assist Visit (SAV) program assesses if commands' entry/exit inspections are conducted and a record of the inspection is maintained. SSO Navy's web portal provides the DoD-5105.21-M-1 self-inspection and DIA SCIF inspection checklist to ensure compliance with all SCI policies and procedures.

- Training is provided through classroom, computer based training, and conferences/seminars. Other training options available for DON SCI security professionals include courses offered through the Defense Security Service Academy (DSSA), and resident and mobile training offered through DIA and ODNI training courses.

- Unlike the rescinded Director Central Intelligence Directive (DCID) 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities, the Intelligence Community Directive (ICD) Number 705 Sensitive Compartmented Information Facilities (SCIFs) series does not mandate a standard for entry/exit inspections; however, the Intelligence Community Standard Number 705 (series number not yet assigned), Technical Specifications draft policy, identifies that command guidance for personnel and package inspections should be addressed in the content of a Standard Operating Procedure (SOP). Further, for visitor access, screening and inspections procedures shall be documented and approved by the Action Officer. The DON Intelligence Community Physical Security Working Group representative for the ICD 705 will ensure entry/exit inspection for SCIF policy language is inserted in the ODNI guidance.

- Entry/exit inspections are not required for open storage of collateral information (i.e., Confidential, Secret, Top Secret). However, safeguarding is required at all levels for collateral information and accountability of Top Secret information is required.

Area of concern: Commanders, supervisors, and individual service members are aware of their responsibilities for the continuing assessment of the trustworthiness of individuals with security clearances and access to classified or sensitive information.

Finding:

- This is required as part of Indoctrination, Orientation, and Annual Refresher briefings. It is also an inherent responsibility of those not only holding a security clearance, but also personnel that work with or supervise personnel with a clearance, to report information under the Continuous Evaluation Program. Additionally, it is required to ensure that the performance rating systems of all DON military and civilian personnel, whose duties significantly involve the creation, handling, or management of classified information, include a critical security element on which to be evaluated. This was recently reinforced by the Under Secretary of the Navy.

- In support of the Continuous Evaluation Program and to promote general awareness of the importance of protecting classified information, DON is developing a communication strategy targeted to reach relevant audiences (e.g., personnel that routinely work with classified material) to generate awareness on policy, proposed changes in policy or procedures, and real world affects of failure to abide by policy and procedures with respect to safeguarding classified or Controlled Unclassified Information (CUI). Additionally, training programs are being reviewed to incorporate the effects of Internet Based Capabilities (i.e. Social networking, FACEBOOK, Twitter, etc.) and associated threats to National Security through an unauthorized disclosure of classified National Security Information (NSI). Intent is to drive user behavior and promote a cultural change, instilling a balance between information sharing and security – to include the insider threat. Leveraging from existing training curricula, DON will ensure training programs incorporate information sharing with the various aspects of Information Security, Information Assurance (IA) and Operations Security (OPSEC), specifically when used with Internet Based Capabilities. Once implemented, training will be required prior to granting network access and annually thereafter.

For the SCI community:

- The DON SCI policy directs each local SCI security official (SSO) with the responsibility to establish a continuing security awareness program that provides frequent exposure of SCI-indoctrinated personnel to security awareness material and designs the program to meet the particular needs of the organization. Security refresher briefings are required at least annually for all persons granted SCI access and are reminded of their continuing security responsibilities. Further, the Navy intelligence community utilizes security newsletters and the SSO Navy web portal to provide periodic security awareness reminders.

- SSO Navy has developed the Senior Intelligence Officer (SIO) training program through CBT and/or resident training courses. DON SIOs are trained in their responsibilities for the overall management of SCI programs within their command. The SIO is responsible for ensuring only those personnel with valid operational requirements for SCI access are considered for SCI clearance and ensures all appointees receive training to perform their respective duties.

- Defense Security Service (DSS) has developed a guide for supervisors for their roles and responsibilities for personnel security. The Office of Director of National Intelligence/Special Security Center (DNI/SSC) provides the Senior Security Professional Seminar (SSPS) for GS-14/15 level. Each provides guidance for continuous evaluation.

- The DON command leadership schools generally lack training and specific discussion topics for Prospective Commanding Officer/Prospective Executive Officer roles and responsibilities for the SCI security program relating to security disciplines (i.e., personnel security and information security). The lack of resources to focus on a well developed and solid SCI security education program prevents program improvement and growth. To mitigate this, the Naval intelligence community has made security awareness, education, and training 2011 priorities. This includes collaboration with applicable training commands, increasing awareness and understanding of the SCI security program.

Area of concern: Information related to a behavioral health evaluation of a service member that may indicate a potential security risk or other "insider threat" may be shared with the Sailor/Marine's chain of command to the greatest extent permitted by law.

Finding:

- Directive-Type Memorandum (DTM) 09-006
  - Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel
- DoD 6025.18-R, Health Information Privacy Regulation, Section C7.11
  - Per the above policy, protected health information may be used and disclosed without an individual's authorization or permission for certain essential government functions including assuring proper execution of a military mission and conducting intelligence and national security activities that are authorized by law. Disclosure may also be made to prevent or lesson a serious and imminent threat to health or safety (Section C7.10).

Policy is promulgated through internship and residency training programs, regular training of all clinical staff, and to mental health communities via their Specialty Leaders.