DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

AUG 14 2014

SECNAV ADMIN
2014 AUG 15 AM 8:01

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Unauthorized Disclosures of Classified Information or Controlled Unclassified Information on DoD Information Systems

The unauthorized disclosure of classified information or controlled unclassified information (CUI) poses a significant threat to our Nation's security and to DoD operations and missions. Safeguarding our classified information and CUI must be the cornerstone of everything we do on all of our information systems, and in every workplace. Accordingly, the attached information safeguarding requirements and incident response measures must be implemented across the Department upon issuance of this memorandum. The attachment also directs the adoption of the term "Negligent Discharge of Classified Information" (NDCI) to connote the seriousness of classified security violations and reinforces the use of appropriate disciplinary and corrective actions in response to such incidents.

Senior leaders, commanders, and supervisors shall ensure that the attached requirements are implemented through appropriate training, accountability, and leadership involvement in these matters. Your personal engagement is essential to foster a culture of increased diligence in safeguarding our classified information and CUI.

Attachment:
As stated

OSD005890-14

ATTACHMENT

INFORMATION SAFEGUARDING REQUIREMENTS AND INCIDENT RESPONSE MEASURES FOR UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION OR CONTROLLED UNCLASSIFIED INFORMATION

References: (a) DoD Manual 5200.01, "Information Security Program," Volumes 1-4
(b) DoD Directive O-8530.1, "Computer Network Defense (CND)," March 9, 2001
(c) Committee for National Security Systems Policy No. 18, "National Policy On Classified Information Spillage," June 2006
(d) Committee for National Security Systems Instruction No. 1001, "National Instruction On Classified Information Spillage," February 2008
(e) Under Secretary of Defense for Intelligence Memorandum, "Processing Classified Information on Information Systems," April 9, 2012
(f) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(g) Under Secretary of Defense for Intelligence Memorandum, "DoD Security Lexicon," June 13, 2013
(h) DoD Directive 5210.50, "Unauthorized Disclosure of Classified Information to the Public," July 22, 2005
(i) Under Secretary of Defense for Intelligence Memorandum, "Amplifying Guidance for Marking and Protecting DoD Information," May 21, 2014

DoD Components will develop, implement, and enforce procedures to prevent the unauthorized disclosure of classified information and controlled unclassified information (CUI) on DoD information systems, to include through compliance with References (a) through (i). DoD and Component-level guidance, policies, and training must include the following:

1. All authorized users of DoD information systems (e.g., DoD civilian employees and military members, other federal agency personnel, DoD contractors), must understand and comply with policy and guidance to protect classified information and CUI, and to prevent unauthorized disclosures. DoD Components will ensure that appropriate requirements are applied to all authorized users (e.g., through DoD issuances, interagency agreements, acquisition regulations, contract requirements).

2. Classified information shall be processed only on information systems approved for such use at the required level of classification, in accordance with References (e), (f) and (i). Additionally:

a. Sensitive Compartmented Information (SCI), e.g., intelligence information marked with SI, TK, or HCS handling caveats, shall be processed only on information systems specifically authorized for SCI processing. The Joint Worldwide Intelligence Communications System (JWICS) is authorized and approved for processing information up to Top Secret/SCI.

b. The Secret Internet Protocol Router Network (SIPRNET) is authorized for processing classified information up to collateral Secret only. SCI, regardless of its classification, may not be processed on, transferred to, or stored on SIPRNET, as that system is not authorized for SCI processing.

3. CUI requires protective measures and controls over access and distribution in accordance with Reference (a), Volume 4, and References (f) and (i).

4. Data spillages and unauthorized disclosures must be aggressively monitored, and commanders and supervisors at all levels shall investigate and, when they deem appropriate, discipline those found to have caused or contributed to such incidents.

a. A spillage occurs whenever classified information or CUI is transferred onto an information system not authorized for the appropriate security level or not having the required CUI protection or access controls. A spillage creates the potential for further widespread unauthorized disclosure of that information, including to the Internet.

b. A classified information spillage is a security violation that is to be investigated, reported, and tracked in accordance with Reference (a), Volume 3, Enclosures 6 and 7. The investigation must determine whether the spill was willful, negligent, or inadvertent.

c. A negligent spillage or unauthorized disclosure of classified information is categorized as a Negligent Discharge of Classified Information (NDCI), which is based on the familiar firearms term "Negligent Discharge," to connote its seriousness. NDCI will be included in the next update to Reference (g).

5. Unauthorized disclosure or spillage of CUI will be handled in accordance with Reference (a), Volume 4, and any amplifying protection and handling guidance for specific types of CUI required by law or federal regulation.

6. Training on procedures to protect classified information and CUI, including Privacy Act information such as Personally Identifiable Information (PII), will be provided to all authorized users during initial indoctrination, annually, and as re-indoctrination briefings in response to incidents.

7. Users will review e-mails, source documents, and information transferred between security domains (e.g., classified to unclassified information system) for the presence of classified information that exceeds an information system's authorized security level, as well as for CUI that is not properly protected (e.g., e-mail containing PII that is not encrypted). In accordance with Reference (a), Volume 1, users shall also consider and verify whether a compilation of information reveals an additional association or relationship that qualifies for higher classification than the individual source documents.

8. The Heads of the DoD Components shall initiate security inquiries into all spillages of classified information in accordance with Reference (a), Volume 3, Enclosure 6, and provide a copy of the preliminary inquiry or investigation to the DoD Component Security Manager and the commander or senior leader of the organization responsible for causing the spillage.

9. The DoD component responsible for a willful or negligent spillage of classified information (e.g., spillage caused by the civilian and military personnel, support contractors, or other federal agency personnel supporting the component) will pay the reimbursable enterprise service providers, in accordance with service level agreements which shall include such provisions, for the associated cleanup costs across the enterprise to restore the affected network(s) to a normal operating

configuration. Individuals who willfully or negligently spill certain types of CUI should be made aware that civil penalties may apply.

10. Commanders and supervisors at all levels must consider and implement, at their discretion, appropriate administrative, judicial, contractual, or other disciplinary/corrective actions in any case related to the improper handling of classified information or CUI, or improper use of information systems. Commanders and supervisors should consult with their legal offices and personnel offices regarding the potential discipline of DoD users, and other available actions regarding non-DoD users, that are responsible for willful or negligent spillages or unauthorized disclosures.

a. Spillages and unauthorized disclosures of classified information or CUI will be categorized in one of three categories:

- Willful. An incident is willful if the person purposefully disregards DoD security or information safeguarding policies or requirements (e.g., intentionally bypassing a known security control).

- Negligent. An incident is negligent if the person acted unreasonably in causing the spillage or unauthorized disclosure (e.g., a careless lack of attention to detail, or reckless disregard for proper procedures).

- Inadvertent. An incident is inadvertent if the person did not know, and had no reasonable basis to know, that the security violation or unauthorized disclosure was occurring (e.g., the person reasonably relied on improper markings).

b. Commanders and supervisors will, as they deem appropriate, suspend user accounts for willful violations or NDCI while corrective actions are pending. Prior to reinstatement of user privileges, the offender will be required to complete corrective training tailored to the nature of the incident.

c. For those individuals who have been the subjects of a national security investigation and who are in the Joint Personnel Adjudication System (JPAS), derogatory information (e.g., a willful unauthorized disclosure or NDCI) will be entered into JPAS and transmitted to the DoD Consolidated Adjudication Facility upon completion of preliminary inquiry or investigation. Commanders and supervisors will report investigation outcomes and corrective actions in JPAS upon completion of the preliminary inquiry or investigation, and ensure a closure report is submitted through their chain of command in accordance with DoD Component guidance. Reporting of derogatory information pertaining to incidents involving non-DoD users will be made pursuant to authorities and procedures governing such users' authorized access to DoD information systems.