UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

ACTION MEMO

DSD 9/7/04

MEMORANDUM FOR SECRETARY OF DEFENSE

FROM: UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AUG 30

SUBJECT: All DoD Activity Message Emphasizing the Principles of Classification at the Request of the Director, Information Security Oversight Office

TAB A reminds the Department of the fundamental principles of classification and directs this office, as the senior security official and proponent for TAB B, to issue minimum training requirements and corrective action. TAB B implements Executive Order 12958, as amended, "Classified National Security Information" requirements for classifying, declassifying and marking classified national security information (TAB C).

TAB A is necessary in view of recent exposes in the public media of questionable classification of DoD documents. The Director, Information Security Oversight Office, responsible for implementation of Executive Order 12958 within the Executive Branch (TAB D) has requested the Secretary take such action and correct the perception that DoD Components are classifying information in violation of EO 12958, as amended.

RECOMMENDATION: ~~Sign the message at TAB A.~~ Approve Message at TAB A.

COORDINATION: OGC

Approved

Disapproved

SEP 9 2004

OSD 13507-04

R 0121302 SEP 04
FM SECDEF WASHINGTON DC
TO ALDODACT
BT
UNCLAS
SUBJ: DoD Information Security Program
ALDODACT XX/04
ADDRESSEES PASS TO ALL SUBORDINATE COMMANDS

Ref: (a) Executive Order 12958, as amended, "Classified National Security Information"
(b) DoD 5200.1-R, "Information Security Program"

1. The President established a strong information security program in Executive Order 12958 (reference a), implemented within the Department by reference (b). Original classification authorities (OCA), designated pursuant to reference (a), and derivative classifiers, are accountable for the accuracy of their classification decisions. Officials with command signature authority shall ensure that classification markings are correct.

2. It is important to state that classifiers shall not: a) use classification to conceal violations of law, inefficiency, or administrative error; b) classify information to prevent embarrassment to a person, organization, or agency; c) classify information to prevent or delay the release of information that does not require protection in the interest of national security. Information may only be classified if it meets the requirements established by the President in reference (a) and reiterated in reference (b).

3. The Under Secretary of Defense for Intelligence (USD(I)) shall issue minimum training requirements for OCAs and derivative classification authorities

within 45 days. USD(I) also shall ensure that security classification guidance is updated, corrective action is taken, as appropriate, at DoD components that generate information related to detainees and prisoner abuse, and that all DoD Components conduct active oversight of all OCA positions for justification to maintain this authority.

4. All classified drafts and working papers shall be clearly marked as such and classification markings applied as required by reference (b). Drafts and working papers may not be used as sources for derivative classification purposes.

5. Any questions should be sent via the chain of command to one of the Military Department's senior security official, the Director of Management, Joint Staff or the Director, Security, (ODUSD/CI&S).

SecDef All DoD Activity Msg

Subj: DoD Information Security Program

Ref: (a) Executive Order 12958, as amended, "Classifie(Nationa Security Information"
(b) DoD 5200.1-R, "Information Security Program"

1. The President strengthened the information security program by amending Executive Order 12958 (reference a), implemented within the Department by reference (b). Original classification authorities (OCA), designated pursuant to reference (a), and individuals who mark documents as classified based on source documents (derivative classifiers), are accountable for the accuracy of their classification decisions. Officials with command signature authority shall ensure that classification markings are correct.
2. The EO mandates that classifiers not: a) use classification to conceal violations of law, inefficiency, or administrative error; b) classify information to prevent embarrassment to a person, organization, or agency; c) classify information to prevent or delay the release of information that does not require protection in the interest of national security. Information may only be classified if it meets the requirements established by the President in reference (a) and reiterated in reference (b).
3. The Under Secretary of Defense for Intelligence (USD(I)) shall re-issue minimum training requirements for OCAs and derivative classification authorities within 60 days. USD(I) also shall ensure that security classification guidance is updated, corrective action is taken, as appropriate, at DoD components that generate information related to detainees and prisoner abuse, and that all DoD Components conduct active oversight of all OCA positions for justification to maintain this authority.
4. All classified drafts and working papers shall be clearly marked as such and classification markings applied as required by reference (b). Drafts and working papers may not be used as sources to classify other documents.
5. Any questions should be sent via the chain of command to one of the Military Department's senior security officials; the Director of Management, Joint Staff; or the Director, Security, (ODUSD/CI&S).

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

January 14, 1997

FOREWORD

This Regulation is issued under the authority of DoD Directive 5200.1, "DoD Information Security Program," December 13, 1996. It prescribes procedures for implementation of Executive Order 12958, "Classified National Security Information," April 20, 1995, within the Department of Defense.

DoD 5200.1-R, "DoD Information Security Program," June 1986, is hereby canceled.

This Regulation applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Uniformed Services University of the Health Sciences, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

This Regulation is effective immediately and is mandatory for use by all the DoD Components. The Heads of the DoD Components may issue implementing instructions when necessary to provide for internal administration of this Regulation within their respective Components.

Send recommended changes to this Regulation through channels to:

Principal Director, Information Warfare, Security and Counterintelligence
Office of the Assistant Secretary of Defense
Command, Control, Communications, and Intelligence
6000 Defense Pentagon
Washington, DC 20301-6000

The DoD Components may obtain copies of this Regulation through their own publication channels. This Regulation will be published in Title 32, Code of Federal Regulations (CPR), Part

These requirements will be revised / strengthened, as necessary.

C9. CHAPTER9

SECURITY EDUCATION AND TRAINING

C9.1. POLICY

C9.1.1. General Policy. Heads of DoD Components shall ensure that personnel of their organization receive such security education and training as may be required to:

C9.1.1.1. Provide necessary knowledge and information to enable quality performance of security functions;

C9.1.1.2. Promote understanding of Information Security Program policies and requirements and their importance to the national security;

C9.1.1.3. Instill and maintain continuing awareness of security requirements and the intelligence threat; and

C9.1.1.4. Assist in promoting a high degree of motivation to support program goals.

C9.1.2. Methodology. Security education and training may be accomplished through establishment of programs within the Component, use of external resources such as the Department of Defense Security Institute, or a combination of the two.

C9.2. INITIAL ORIENTATION

C9.2.1. Cleared Personnel

C9.2.1.1. All personnel in the organization who are cleared for access to classified information shall be provided an initial orientation to the Information Security Program before being allowed access to classified information. This initial orientation is intended to produce a basic understanding of the nature of classified information and the importance of its protection to the national security, place employees on notice of their responsibility to play a role in the security program, and provide them enough information to ensure proper protection of classified information in their possession. Security educators should consider including:

C9.2.1.1.3.5. What steps should be taken in an emergency evacuation situation?

C9.2.1.1.3.6. What are the appropriate policies and procedures for transmission of classified information?

C9.2.1.2. Before being granted access to classified information, employees must sign Standard Form 312, "Classified Information Nondisclosure Agreement." Cleared personnel who have signed an earlier nondisclosure agreement, the SF 189, need not sign SF 312, but they may elect to replace their SF 189 with a signed SF 312. SFs 189 and 312 shall be maintained for 50 years from the date of signature.

C9.2.2. Uncleared Personnel. Members of the organization who are not cleared for access to classified information should be included in the security education program if they will be worlung in situations where inadvertent access to classified information might occur or will have access to unclassified information that might be of value to intelligence collectors. They should be provided with a brief explanation of the nature and importance of classified information and actions they should take if they discover classified information unsecured, note an apparent security vulnerability, or believe they are contacted by an intelligence collector.

C9.3. SPECIAL REQUIREMENTS

C9.3.1. General. Members of the organization in positions that require performance of specified roles in the Information Security Program shall be provided security education and training sufficient to permit quality performance of those duties. The education and training shall be provided before, concurrent with, or not later than 6 months following assumption of those positions.

C9.3.2. Original Classifiers. The security education and training provided to original classification authorities shall, as a minimum, address each of the following:

C9.3.2.1. What is the difference between original and derivative Classification?

C9.3.2.2. Who can classify information originally?

C9.3.2.3. What are the standards that an original classifier must meet to classify information?

C9.3.2.4. What is the process far determining duration of classification?

C9.3.2.5. What are the prohibitions and limitations on classifying information?

C9.3.2.6. What are the basic markings that must appear on classified information?

C9.3.2.7. What are the general standards and procedures for declassification?

C9.3.2.8. What are the requirements and standard for creating, maintaining and publishing security classification guides?

C9.3.3. Declassification Authorities Other Than Original Classifiers. The security education and training provided declassification authorities other than original classifiers shall, as a minimum, address each of the following:

C9.3.3.1. What are the standards, methods and procedures for declassifying information under Executive Order 12958 (reference (e)) and this Regulation?

C9.3.3.2. What are the standards for creating and using declassification guides?

C9.3.3.3. What is contained in the Component's declassification plan?

C9.3.3.4. What are the Component's responsibilities for the establishment and maintenance of a declassification database?

C9.3.4. Derivative Classifiers, Security Personnel and Others. Individuals specifically designated as responsible for derivative classification, security managers, classification management officers, security specialists or any other personnel whose duties significantly involve the management and oversight of classified information shall receive training that, as a minimum, addresses the following:

C9.3.4.1. What are the original and derivative classification processes and the standards applicable to each?

C9.3.4.2. What are the proper and complete classification markings to be applied to classified information?

C9.3.4.3. What are the authorities, methods and processes for downgrading and declassifying information?

C9.3.4.4. What are the methods for the proper use, storage, reproduction, transmission, dissemination and destruction of classified information?

C9.4. CONTINUING SECURITY EDUCATION/REFRESHER TRAINING

C9.4.1. Continuing Security Education. Security education should be a continuous, rather than a periodic influence on individual security performance. Periodic briefings, training sessions, and other formal presentations should be supplemented with other information and promotional efforts to ensure maintenance of continuous awareness and performance quality. The use of job performance aids and other substitutes for formal training is encouraged when they are determined to be the most effective means of achieving program goals. The circulation of directives or similar material on a "read-and initial"basis shall not be considered as a sole means of fulfilling any of the specific requirements of this Chapter.

C9.4.2. Refresher Training. **As** a minimum, personnel shall receive annual refresher training that reinforces the policies, principles and procedures covered in initial and specialized training. Refresher training should also address the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Refresher training should also address issues or concerns identified during Component self-inspections.

C9.5. TERMINATION BRIEFINGS

C9.5.1. General. The DoD Components shall establish procedures to ensure that cleared employees who leave the organization or whose clearance is terminated receive a termination briefing. This briefing shall emphasize their continued responsibility to:

C9.5.1.1. Protect classified information to which they have had access;

C9.5.1.2. Provide instructions for reporting any unauthorized attempt to gain access to such information;

C9.5.1.3. Advise the individuals of the prohibition against retaining material when leaving the organization; and

C9.5.1.4. Remind them of the potential civil and criminal penalties for failure to fulfill their continuing security responsibilities.

C9.6. PROGRAM OVERSIGHT

Heads of the DoD Components shall ensure that security education programs are appropriately evaluated during self-inspections and other oversight activities. This evaluation shall include assessment of the quality and effectiveness of security education efforts, as well as ensuring appropriate coverage of the target populations. Heads of the Components shall require maintenance of whatever records of programs offered **and** employee participation they deem necessary to permit effective oversight.

Federal Register
Vol. 68, No. 60
Friday. March 28, 2003

Presidential Documents

Title 3—

The President

Executive Order 13292 of March 25, 2003

Further Amendment to Executive Order 12958, as Amended, Classified National Security Information

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to further amend Executive Order 12958, as amended, it is hereby ordered that Executive Order 12958 is amended to read as follows:

"Classified National Security Information

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security remains a priority.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1—ORIGINAL CLASSIFICATION

Sec. 1.1. *Classification Standards.* (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of informaiion listed in section 1.4 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

(b) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

(c) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

Sec. 1.2. *Classification Levels.* (a) Information may be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the

national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

Sec. **1.3.** Classification Authority. (a) The authority to classify information originally may be exercised only by:

(1) the President and, in the performance of executive duties, the Vice President;

(2) agency heads and officials designated by the President in the Federal **Register;** and

(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President; in the performance of executive duties, the Vice Presidsnt; or an agency head or official designated pursuant to paragraph (a)(2) of this section.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President: in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to paragraph (a)(2) of this section; or the senior agency official described in section 5.4(d) of this order, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives. Such training must include instruction on the proper safeguarding of classified information and of the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure.

(e) Exceptional cases. When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within **30** days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.4. *Classification Categories.* Information shall not be considered for classification unless it concerns:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

(h) weapons of mass destruction.

Sec. 1.5. *Duration of Classification.* (a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. The date or event shall not exceed the time frame established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it shall be marked for declassification for up to 25 years from the date of the original decision. All information classified under this section shall be subject to section 3.3 of this order if it is contained in records of permanent historical value under title 44, United States Code.

(c) An original classification authority may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) Information marked for an indefinite duration of classification under predecessor orders, for example, marked as "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordarice with part 3 of this order.

Sec. 1.6. *Identification and Markings.* (a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) one of the three classification levels defined in section 1.2 of this order;

(2) the identity, by name or personal identifier and position, of the original classification authority:

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.5(a) or section 1.5(c);

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b); or

(C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5(b); and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.4 of this order.

(b) Specific information described in paragraph (a) of this section may be excluded if it would reveal additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

(h) Prior to public release, all declassified records shall be appropriarely marked to reflect their declassification.

Sec. **1.7.** *Classification Prohibitions and Limitations.*

(a) In no case shall information be classified in order tu:

(1) conceal violations of law, inefficiency, or administrative error;

(2) prevent embarrassment to a person, organization, or agency:

(3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of the national security.

(b) Basic scientific research information not clearly related to the national security shall not be classified.

(c) Information may be reclassified after declassification and release to the public under proper authority only in accordance with the following conditions:

(1) the reclassification action is taken under the personal authority of the agency head or deputy agency head, who determines in writing that the reclassification of the information is necessary in the interest of the national security;

(2) the information may be reasonably recovered; and

(3) the reclassification action is reported promptly to the Director **of** the Information Security Oversight Office.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section **3.5** of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with

(3) limits the access granted to former Presidential appointees and Vice Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee or a Vice Presidential appointee.

PART 5—IMPLEMENTATION AND REVIEW

Sec. 5.1. *Program Direction.* (a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the Assistant to the President for National Security Affairs, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

(1) classification and marking principles;

(2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;

(3) agency security education and training programs;

(4) agency self-inspection programs; and

(5) classification and declassification guides.

(b) The Archivist shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

Sec. 5.2. *Information Security Oversight Office.* (a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Archivist, acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

(2) oversee agency actions to ensure compliance with this order and its implementing directives;

(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the President through the Assistant to the President for National Security Affairs within 60 days of the request for access. Access shall be denied pending the response;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Assistant to the President for National Security Affairs;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

COORDINATION

SUBJECT: All DoD Activity Message Emphasizing the Principles of Classification at the Request of the Director, Information Security Oversight Office

OSD/OGC	D. Dell'Orto	Concur	**23** Aug 04