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

APR 16 2004

REC'D CNO (N09N2)
13 MAY 2004

INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
COMMANDERS OF THE COMBATANT COMMANDS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DOD FIELD ACTIVITIES
DIRECTOR, ADMINISTRATION AND MANAGEMENT

SUBJECT: Interim Information Security Guidance

This directive-type memorandum provides interim guidance on changes to DoD Regulation 5200.1, "Information Security Program," dated January 1997. Attachment 1 implements changes required by Executive Order (EO) 12958, as amended, "Classified National Security Information," and the Information Security Oversight Office (ISOO) "Classified National Security Information Directive No. 1." Attachment 2 provides interim guidance on security containers, classified conferences, and controlled unclassified information requirements.

The attached interim guidance is effective immediately. Please ensure widest dissemination. DoD 5200.1-R will be updated within 180 days to reflect these changes.

Our point of contact is Mrs. Deborah Ross at 703-695-2686 or e-mail: deborah.ross@osd.mil.

for Stephen A. Cambone

Attachments
As stated

INTERIM GUIDANCE
ON CHANGES TO
EXECUTIVE ORDER 12958, AS AMENDED
AND
ISOO DIRECTIVE NO. 1

TABLE OF CONTENTS

Subject	Page
GENERAL	1
KEY HIGHLIGHTS	1-2
CHAPTER 2: ORIGINAL CLASSIFICATION	
1. Classification Categories Revised	2-3
2. Level of Classification	3
3. Duration of Classification	3-4
4. Reclassification of Information that Has Not Been Released to the Public Under Proper Authority	4-5
5. Reclassification of Information that Has Been Released to the Public Under Proper Authority	5-6
6. Security Classification and/or Declassification Guides	7
CHAPTER 3: DERIVATIVE CLASSIFICATION	7
CHAPTER 4: DECLASSIFICATION AND REGRADING	
1. Declassification Without Proper Authority	7
2. Automatic Declassification	7-13

3. Restricted Data and Formerly Restricted Data 13

4. Mandatory Declassification Review Processing Time 13

5. Referrals 13-16

6. Public Release of Automatically Declassified Documents 16

7. Integral File Block 16

CHAPTER 5: MARKING

1. Original Classification Markings 16-17

2. Derivative Classification Markings 17-18

3. Automatic Declassification Exemption Markings 18-19

4. Declassification Markings 19-20

5. Reclassification Markings 20-21

CHAPTER 6: SAFEGUARDING

1. Emergency Authority 21-22

APPENDIX 2: DEFINITIONS 22-24

INTERIM GUIDANCE
FOR CHANGES TO
EXECUTIVE ORDER 12958, AS AMENDED
AND
ISOO DIRECTIVE NO. 1

GENERAL

This Interim Guidance supplements DoD Regulation 5200.1, "Information Security Program," January 1997. It prescribes general implementation of Executive Order (EO) 12958, as amended, "Classified National Security Information" dated 23 March 2003 and the Information Security Oversight Office (ISOO) Directive No. 1, dated 22 September 2003.

The Interim Guidance is listed in the order of the Chapters in DoD 5200.1-R. The official change to the regulation will be forthcoming.

KEY HIGHLIGHTS OF THE REVISIONS:

- Extends the effective date for automatic declassification of information already 25 years old to 31 December 2006;

- Allows for the delay of automatic declassification for certain types of records;

- Clarifies the duration of classification for original classification authorities;

- Incorporates classification of information related to transnational terrorism, critical infrastructure, protection services, and weapons of mass destruction;

- Allows under certain circumstances for the reclassification of specific information even if it has been declassified and released to the public;

- Provides Agencies with the continuing ability to exempt a file series;

- Authorizes Agency heads or designated persons to share classified information in an emergency situation with individuals not otherwise eligible to receive the information;

- Eliminates the 10 year exemption categories (X1 through X8);

- Allows Agencies to propose exempting originally classified information (not already covered by an Information Security Clearance Appeals Panel (ISCAP) exemption) from automatic declassification within five years of, but not later than 180 days before the information is subject to automatic declassification;

- Increases the amount of time Agencies have to respond to a Mandatory Declassification Request; and

- Changes declassification markings, and markings for material exempt from automatic declassification.

CHAPTER 2: ORIGINAL CLASSIFICATION

1. **Classification Categories Revised.** The classification categories are now in Section 1.4 of EO 12958, as amended, versus 1.5 and have been changed to include information related to transnational terrorism, critical infrastructure, weapons of mass destruction, and protection services. Original Classification Authorities (OCA) shall not classify information 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.

(EO 12958, as amended, Section 1.4.)

2. **Level of Classification.** Section 1.3(c) of the 1995 EO 12958 stating that "if there is significant doubt about the appropriate level of classification, it shall be classified at the lower level" has been removed from EO 12958, as amended.

3. **Duration of Classification.**

(a) Duration Options. The 10-year exemption (categories X1 through X8) from automatic declassification is no longer an option for original classifiers to use as a declassification instruction. Instead, an OCA has two options for duration of classification, as follows:

(1) An OCA shall apply a date or event 25 years or less from the date of the information, or

(2) An OCA shall apply the 25X1-human exemption with no date of declassification when classifying information that could be expected to reveal the identity of a confidential human source or human intelligence source. Only OCAs having jurisdiction over such information may originally classify it.

Note: OCAs shall ensure that ISCAP-approved exemptions relevant to their programs are cited in the appropriate security classification guides.

(ISOO Directive No. 1, Section 2001.12(a)(1)-(2))

(b) Extending Classification Beyond 25 Years for Information in Records Determined Not to Have Permanent Historical Value. For information determined not to have permanent historical value, the duration of classification beyond 25 years shall be the same as the disposition of those records in each Military Department's and other DoD Component's Records Control Schedule or General Records Schedule approved by the National Archives and Records Administration, although the duration of classification may be extended if a record has been retained for business reasons beyond its scheduled destruction date.

(ISOO Directive No. 1, Section 2001:12(a)(2)(ii))

(c) Extending Classification Beyond 25 Years for Unscheduled Records. For unscheduled classified records (both permanent and temporary), the duration of classification beyond 25 years shall be determined when the records are scheduled.

(ISOO Directive No. 1, Section 2001.12(a)(2)(iii))

(d) Changing the Classification Level of Information Originally Classified under the Order. An OCA may change the level of classification of information under their jurisdiction. Documents shall be remarked with the new classification level, the date of the action, and the authority for the change. Changing the classification level may also require changing portion markings for information contained within a document. Additionally, the OCA shall update appropriate security classification guides and immediately notify all holders of the information of the changes.

(ISOO Directive No. 1, Section 2001.12(c))

4. **Reclassification of Information that Has Not Been Released to the Public Under Proper Authority.** Classified information that has been released to the public without proper authority may remain classified if the appropriate OCA makes a determination that it should.

(a) When the determination is made that the information will remain classified, the appropriate OCA will notify holders accordingly and provide the following marking guidance to be used in the event the information is not marked:

(1) Overall level of classification:

(2) New portion markings;

(3) Identity, by name or personal identifier and position, of the OCA;

(4) Declassification instructions;

(5) Concise reason for classification; and,

(6) Date the action was taken.

(ISOO Directive No. 1, Section 2001.12(d))

5. **Reclassification of Information that Has Been Released to the Public Under Proper Authority.**

(a) In making the decision to reclassify information that has been declassified and released to the public under proper authority, the Military Departments and other DoD Component Heads or their Deputy Heads must determine in writing that reclassification of the information is necessary in the interest of the national security. Military Department Heads or their Deputy Heads make the decision to reclassify information under their jurisdiction. Other DoD Component Heads or their Deputy Heads must submit requests to reclassify such information under their jurisdiction through established channels to DUSD(CI&S). Requests must include:

(1) A description of the information.

(2) The classification level of the information.

(3) When and how it was released to the public.

(4) An explanation as to why it should remain classified. Include the applicable EO 12958, as amended, reason and describe what damage could occur to national security. Also describe what damage may have already occurred as a result of the release.

(5) The number of recipients/holders and how they will be notified of the reclassification.

(6) How the information will be recovered.

(b) In addition, the DoD Components and Military Departments must deem the information to be reasonably recoverable which means that:

(1) Most individual recipients or holders are known and can be contacted and all forms of the information to be reclassified can be retrieved from them.

(2) If the information has been made available to the public via means such as Government archives or reading rooms, it is withdrawn from public access.

(c) The declassification and release of information under proper authority means that the OCA originating the information authorized the declassification and release of the information.

(d) Once the reclassification action has occurred, it must be reported to all recipients/holders and the ISOO within 30 days. The notification to ISOO must include how the "reasonably recoverable" decision was made including the number of recipients or holders, how the information was recovered and how the recipients or holders were notified/briefed. Military Department Agency Heads or their Deputy Agency Heads will notify ISOO directly and provide an information copy to DUSD(CI&S). DUSD(CI&S) will notify ISOO for the other DoD Components.

(e) Any cleared recipients or holders of the reclassified information shall be notified and appropriately briefed about their continuing legal obligations and responsibilities to protect this information from unauthorized disclosure. The recipients or holders who do not have security clearances shall, to the extent practicable, be appropriately briefed about the reclassification of the information that they have had access to and their obligation not to disclose the information, and be requested to sign an acknowledgement of the briefing.

(f) The reclassified information must be marked according to Chapter 5 and safeguarded in accordance with DoD 5200.1-R.

(ISOO Directive No. 1, Section 2001.13)

6. **Security Classification and/or Declassification Guides.**

(a) General Content of Classification Guides: Military Departments and other DoD Components may incorporate declassification guidance from ISCAP approved declassification guides or file series exemptions into revised or updated versions of applicable security classification guides. For files series exemptions, also see Chapter 5, paragraph 3(b).

(ISOO Directive No. 1, Section 2001.15(b)(8))

(b) Declassification Guides Pending ISCAP Approval. Military Departments and other DoD Components that have submitted a declassification guide to the ISCAP may not apply the 25X markings until ISCAP has approved the exemptions or the Panel's Executive Secretary permits it.

(ISOO Directive No. 1, Section 2001.32(c))

CHAPTER 3: DERIVATIVE CLASSIFICATION

See Chapter 5 for changes to derivative marking requirements.

CHAPTER 4: DECLASSIFICATION AND REGRADING

1. **Declassification Without Proper Authority**. Classified information that has been declassified without proper authority remains classified. Administrative action shall be taken to restore markings and controls, as appropriate. Also see reclassification policy in Chapter 2, paragraphs 4 and 5.

(ISOO Directive No. 1, Section 2001.10(d))

2. **Automatic Declassification.**

(a) Information Marked with 10-Year Exemption Categories. Information marked with exemption categories X1 through X8 prior to 22 September

2003, shall be automatically declassified 25 years from the date of the original decision, unless it has been exempted according to subparagraph (e) below.

(ISOO Directive No. 1, Section 2001.12(a)(1)-(2) and Section 2001.12(e))

(b) Classified Information in the Custody of Contractors, Licensees, Certificate Holders, Grantees or Other Authorized Private Organizations or Individuals. Pursuant to the provisions of the National Industrial Security Program, Military Departments and other DoD Components must provide security classification/declassification guidance to such entities or individuals who possess DoD classified information. Military Departments and other DoD Components must also determine if classified Federal records are held by such entities or individuals, and if so, whether they are permanent records of historical value and thus subject to automatic declassification. Until such a determination has been made by an appropriate official, the classified information contained in such records shall not be subject to automatic declassification and shall be safeguarded in accordance with the most recent security classification/declassification guidance provided by the Military Departments and other DoD Components.

(ISOO Directive No. 1, Section 2001.30(c))

(c) Deadline for Automatic Declassification Extended. Unless exempted, no later than 31 December 2006, all classified records that are more than 25 years old and have been determined to have permanent historical value will be automatically declassified whether or not the records have been reviewed.

(EO 12958, as amended, Section 3.3(a) and ISOO Directive No. 1, Section 2001.30(k))

(d) Delays in the Onset of Automatic Declassification. The following lists the scenarios for which automatic declassification may be delayed.

(1) Microforms, motion pictures, audiotapes, videotapes, or comparable media. A Military Department Agency Head, other DoD Component Agency Head or Senior Agency Official, either through its Agency's declassification plan, or within 90 days of the decision, must notify the Director of ISOO of a decision to delay the onset of automatic declassification for classified information contained in this type of media.

Military Department Agency Heads or their Senior Agency Official will notify ISOO directly and provide an information copy to DUSD(CI&S). Other DoD Component Agency Heads or their Senior Agency Official will notify ISOO through DUSD(CI&S). Military Departments and other DoD Components may delay the date for automatic declassification for up to five additional years for these types of special media. Information contained in special media that has been referred shall be automatically declassified five years from the date of notification or 30 years from the date of origination of the special media, whichever is longer, unless the information has been properly exempted.

(2) Referred or Transferred Records. A Military Department Agency Head, other DoD Component Agency Head, or Senior Agency Official, either through the Agency's declassification plan or within 90 days of the decision, must notify the Director of ISOO of a decision to delay the onset of automatic declassification for records that have been referred or transferred to that Agency. Military Department Agency Heads or their Senior Agency Official will notify ISOO directly and provide an information copy to DUSD(CI&S). Other DoD Components or their Senior Agency Official will notify ISOO through DUSD(CI&S). Military Departments and other DoD Components that have records subject to automatic declassification must identify all equities and refer them to the appropriate Agency prior to the date of automatic declassification or, if the information has been properly exempted by the referring Agency, prior to the specific date or event for declassification. Information contained in records that have been referred shall be automatically declassified three years from the date of notification or 28 years from the date of origination of the records, whichever is longer, unless the information has been properly exempted by another equity holding Agency. Military Departments and other DoD Components receiving a notification of a referral must immediately acknowledge receipt of it. Notifying Military Departments and other DoD Components must follow-up if an acknowledgment is not received within 60 days.

(3) Newly Discovered Records. A Military Department Agency Head, other DoD Component Agency Head, or Senior Agency Official must notify the Director of ISOO of any decision to delay automatic declassification no later than 90 days, from discovery of the records. Military Department Agency Heads or their Senior Agency Official will notify ISOO directly and provide an information copy to DUSD(CI&S). Other DoD Component Agency Heads or their Senior Agency Official will

notify ISOO through the DUSD(CI&S). The notification should identify the records and the anticipated date for declassification. A Military Department or other DoD Component has up to three years from the date of discovery to make a declassification, exemption or referral determination. If other Agencies' interests or equities are identified in the newly discovered records, those Agencies will have three years from the date of notification to complete their review and make a declassification or exemption determination.

(ISOO Directive No. 1, Section 2001.30(m)(1)–(3))

(e) Exemptions from Automatic Declassification. Exemptions from automatic declassification may be obtained on information pertaining to one or more of the exemption categories listed below.

(1) The exemption categories are as follows:

- 25X1: reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

- 25X2: reveal information that would assist in the development or use of weapons of mass destruction;

- 25X3: reveal information that would impair U.S. cryptologic systems or activities;

- 25X4: reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

- 25X5: reveal actual U.S. military war plans that remain in effect;

- 25X6: reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

- 25X7: reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

- 25X8: reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or

- 25X9: violate a statute, treaty, or international agreement.

(EO 12958, as amended, Section 3.3(b)(1)-(9) and ISOO Directive No. 1, Section 2001.21(e)(2))

(2) Exempting Discrete Elements of Information: Military Departments and other DoD Components may propose to exempt from automatic declassification discrete elements of information pertaining to one or more of the exemption categories in paragraph 2(e), either by reference to information in specific records or in the form of a classification or declassification guide, within five years of, but not later than 180 days before the information is subject to automatic declassification. To obtain an exemption for discrete elements of information, Military Department Agency Heads, other DoD Component Agency Heads, or Senior Agency Officials within the specified timeframe, shall notify the Director of ISOO, serving as the Executive Secretary of the ISCAP, of the specific information being proposed for exemption from automatic declassification. Military Department Agency Heads or their Senior Agency Official will notify ISOO directly and provide an information copy to DUSD(CI&S). Other DoD Component Agency Heads or their Senior Agency Official will notify ISOO through DUSD(CI&S).

Note: The following ISCAP approved language will be included in DoD declassification guides used to apply for exemptions on discrete elements of information: "An initial re-review of records containing information exempted by this guide shall occur within [DoD Component specific number] years of the date of ISCAP approval of this guide. Subsequent re-reviews shall occur within [DoD Component specific number] years of the

date of the prior review, using declassification guidance in effect at the time of the re-review. Whenever a scheduled review cannot be conducted, notification will be provided within 90 days to the Director, Information Security Oversight Office through the Under Secretary of Defense (Intelligence). The notification will provide an explanation for why the re-review was not completed and provide a date certain by which the re-review will occur; not more than five years from the date of notification."

(ISOO Directive No. 1, Section 2001.30(l))

(3) Exempting File Series. Military Departments and other DoD Components may propose to exempt from automatic declassification an entire file series if it is replete with information that almost invariably falls within one or more of the exemption categories listed in paragraph 2(e) and which the Military Departments or other DoD Components propose to exempt from automatic declassification. To obtain an exemption for file series, Military Department Agency Heads or their Senior Agency Official will notify the Assistant to the President for National Security Affairs directly and provide an information copy to DUSD(CI&S). Other DoD Component Agency Heads or their Senior Agency Official will notify the Assistant to the President for National Security Affairs through DUSD(CI&S). Notifications shall include:

- a description of the file series;
- an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and,
- except for the identity of a confidential human source or a human intelligence source, as provided in Chapter 2, a specific date or event for declassification of the information. The President may direct Military Department Agency Heads or other DoD Component Agency Heads not to exempt the file series or to declassify the information within that series at an earlier date than recommended. File series exemptions previously approved by the President shall remain valid without any additional DoD Component/Military Department action.

(EO 12958, as amended, Section 3.3(c)(1)-(3))

3. **Restricted Data and Formerly Restricted Data**. Documents marked or containing Restricted Data or Formerly Restricted Data are excluded from the automatic declassification provisions of EO 12958, as amended, and shall remain classified indefinitely or shall be referred to the Department of Energy for a classification review.

(ISOO Directive No. 1, Section 2001.30(o)).

4. **Mandatory Declassification Review Processing Time**. Mandatory review requests must identify the information requested with enough specificity to allow Military Department and other DoD Component personnel to locate the records with a reasonable amount of effort. Military Departments and other DoD Components shall either make a prompt declassification determination to notify the requester accordingly, or inform the requester of the additional time needed to process the request. Military Departments and other DoD Components shall ordinarily make a final determination within one year from the date of receipt. When information cannot be declassified in its entirety, Military Departments and other DoD Components shall make reasonable efforts to release, consistent with other applicable law, those declassified portions of the requested information that constitute a coherent segment.

(ISOO Directive No. 1, Section 2001.33(a)(2)(i))

5. **Referrals**. ISOO Directive No. 1, Appendix A, dated 13 September 1999 established a uniform referral standard. ISOO Directive No. 1 dated 22 September 2003 incorporates the previous guidance on referrals into the main body of the document. The entire section on referrals is provided below. The term Agency for this section applies to the individual Military Departments, other DoD Components, and all Executive Branch Agencies.

(a) Approaches to Declassification. The exchange of information between Agencies and the final disposition of documents are affected by differences in the approaches to declassification. To facilitate this process, the ISOO, in coordination with NARA and the other concerned Agencies, shall standardize the referral process, including the development of standard forms. Agencies conducting pass/fail reviews may refer documents to

Agencies that redact. Actions taken by the sender and the recipient may differ as noted below:

(1) When a referral is from a pass/fail Agency to a pass/fail Agency, both Agencies conduct a pass/fail review and annotate the classification or declassification decisions in accordance with NARA guidelines. The receiving Agency should also notify the referring Agency that the review has been completed.

(2) When a referral is from a pass/fail Agency to a redaction Agency, the redaction Agency is only required to conduct pass/fail reviews of documents referred by a pass/fail Agency. If the redaction Agency wishes to redact the document, it must do so on a copy of the referred document, then file the redacted version with the original. The redaction Agency should also notify the pass/fail referring Agency that the review has been completed.

(3) Referrals from redaction Agencies to pass/fail Agencies will be in the form of document copies. In the course of review the pass/fail Agency may either pass or fail the document or its equities. The pass/fail Agency may review and redact failed documents when practicable.

(4) Referrals between redaction Agencies may result in redaction of any exemptible equities.

(b) Referral Decisions. When Agencies review documents or folders only to the point at which exemptible information is identified, they must take one of the following actions to protect any other unidentified equities that may be in the unreviewed portions of the document:

(1) Complete a review of the document or folder to identify other Agency equities and notify those Agencies; or

(2) Exempt the document or folder and assign a Date/Event for automatic declassification, before which time they must provide timely notification to any equity Agencies. Agencies reviewing a previously exempted document or folder may apply a different exemption and new Date/Event for automatic declassification based upon the content of previously unreviewed equities.

(c) Means of Referral. The reviewing Agency must communicate referrals to equity Agencies. They may use either of the methods below:

(1) *Full Text Referral*. Agencies will make referrals in a format mutually agreed to by the referring and receiving Agencies. Each referral request will clearly identify the referring Agency and may identify the sections or areas of the document containing the receiving Agency's equities and the requested action; or

(2) *Tab and Notify*.

- Agencies will use NARA-approved tabs and will clearly indicate on them the Agency or Agencies having equity in the document(s) held within the tabs. Successive documents with identical equity(ies) may be grouped within a single tab. Documents with differing equities, or non-successive documents, must be tabbed individually. In general, document order may not be changed to facilitate tabbing. In cases where there are so many tabbed documents in a box that tabbing documents individually would seriously overfill the box, the reviewer may group documents under a single tab for each Agency equity at the back of each file folder, or back of the box if there is no file folder. If this becomes necessary, the reviewer shall prepare a folder/document list or consult with NARA so that original order can be restored during archival processing.

- Agency notification must include, at a minimum, the following information: the approximate volume of equity, the highest classification level of the documents, the exact location (to box level) of the documents, and instructions related to access to the boxes containing the documents.

- Agencies will acknowledge receipt of referral notifications. They should notify the referring Agency that the review is complete. Any additional equities noted in the review must be annotated on the tab and brought to the attention of the referring Agency so they can notify those newly identified Agencies.

- Equity Notification Database. Agencies may also use an electronic notification database as a means of notification. Use of such a

database, when available, will constitute referral and acknowledgement of referrals received under the Order.

(ISOO Directive No. 1, Section 2001.34)

6. **Public Release of Automatically Declassified Documents**. Declassified documents will not be released to the public until a public disclosure review per DoD 5230.29, "Security and Policy Review of DoD Information for Public Release," has been conducted to determine if there are other reasons for preventing the release of the information.

7. **Integral File Block.** Classified records within an integral file block that are otherwise subject to automatic declassification under this section shall not be automatically declassified until 31 December of the year that is 25 years from the date of the most recent record within the file block.

(EO 12958, as amended, Section 3.3(e)(1))

CHAPTER 5: MARKING

1. **Original Classification Markings.** There are no changes to the overall classification markings, portion markings, or "Classified By" line. However, the following markings have changed:

(a) "Reason" Line: The reference for this line is now Section 1.4 *not* 1.5 of EO 12958, as amended, along with the applicable classification category shown in Chapter 2, paragraph 1.

(ISOO Directive No. 1, Section 2001.21(a)(3))

(b) "Declassify On" Line: One of the two options described in Chapter 2, paragraph 3 may be applied based on the sensitivity of the information. Note that the only time it is permissible to reflect a "25X" marking in the "Declassify on" line of an originally classified document is when the information falls under the 25X1-human exemption or when in rare instances, newly classified information clearly falls under a pre-existing ISCAP approved exemption.

(c) Examples:

(1) *Showing an event as the declassification instruction.* The source document is dated 10 October 2004, and the information will no longer meet the standards for classification 15 days after Admiral West completes his trip:

Classified by: David Smith, Chief, Protective Services Division, Department of Military Travel
Reason: 1.4(g)
Declassify on: 15 days after Admiral West completes travel to Europe.

(2) *Showing a date less than 25 years as the declassification instruction.* The document is dated 10 October 2003, and the information will no longer meet the standards for classification in eight years:

Classified by: David Smith, Chief, Division 5, Department of Good Works
Reason: 1.4(h)
Declassify on: 10 October 2011

(3) *Showing a 25X exemption code as the declassification instruction.* The document is dated 20 January 2004, but the information in the document is exempt from automatic declassification under an approved declassification guide.

Classified by: F. E. Jones, Commanding General DoD Joint Service Activity
Reason: 1.4(a)
Declassify on: 25X4 and IAW applicable SCG

(ISOO Directive No. 1, Section 2001.21(a)(4))

2. **Derivative Classification Markings**. There was no change in the overall classification markings, portion markings, and "Derived From" line. However, the following markings have changed:

(a) "Declassify On" Line: The derivative classifier shall carry forward to the derivative document the instructions on the "Declassify on" line from the source document or the duration instruction from the security classification

or declassification guide. In those instances where (a) source document(s) contain(s) the declassification instruction "OADR" or "X1 through X8," the derivative classifier, unless otherwise instructed, shall note (1) the fact that the source document(s) was marked with either of these instructions; and (2) the date of origin of the most recent source document as appropriate to the circumstances.

(1) An example of derived declassification instructions obtained from sources with 10-year exemptions cited as the declassification instruction.

- *Using a source document with a 10-year exemption declassification instruction.* The source document used for a derivative decision that is being made on 15 November 2003, has "X4" on the "Declassify on" line. The date of the source document is 2 December 2000.

  Derived from: Department of Weapons Memo dated 2 December 2000, Subject: New LASER Gun
  Declassify on: Source marked X4, Date of Source, 2 December 2000

(2) Note that derivatively classified documents may carry a 25X declassification marking when one or more of the sources used contain 25-year-old information exempted from automatic declassification. Declassifiers shall always refer to the applicable security classification/declassification guide for the most current declassification date.

Derived from: Multiple Sources
Declassify on: 25X4 and IAW applicable SCG

(ISOO Directive No. 1, Section 2001.22)

3. **Automatic Declassification Exemption Markings.**

(a) 25-Year Exemption Marking. The marking applied to information exempted from the 25-year automatic declassification provisions of EO 12958, as amended, cannot be used until the exemption is approved through the ISCAP process or permitted by the Panel's Executive Secretary. When used, the "Declassify on" line would include the symbol "25X" plus a brief

reference to the applicable exemption category(ies) and the statement "IAW applicable SCG." This will help ensure declassifiers go to the correct source for obtaining the most current declassification date. The marking would appear as:

Declassify on: 25X-State-of-the-art use of technology within a U.S. weapons system, and IAW applicable SCG

or

Declassify on: 25X4, and IAW applicable SCG

(b) File Series Exemption Marking. Documents removed from a file series exempted from automatic declassification are marked at the time of removal and in the same manner as 25-year exempted information described in paragraph 3(a) above when it is determined that continued classification is required. As these documents are reviewed and information is identified as requiring continued classification, Military Departments and other DoD Components must incorporate the specific information along with a date or event for declassification into their security classification/declassification guide.

(c) Human Source Exemption Marking. The identity of a confidential human source or a human intelligence source is not subject to automatic declassification when classified by an appropriate OCA. The marking for the exemption of this specific information is:

Declassify on: 25X1-human

Note: Information about the application of an intelligence source or method is still subject to automatic declassification on a specific date or event that must be included on the "Declassify on" line.

(ISOO Directive No. 1, Section 2001.21(e))

4. **Declassification Markings.**

(a) General. A uniform security classification system requires that standard markings be applied to declassified information. The marking of declassified information shall not deviate from the following prescribed

formats unless a waiver has been approved by ISOO. Such requests shall be submitted through DUSD(CI&S). If declassification markings cannot be affixed to specific information or materials (e.g., special media, microfilm, etc.), the originator shall provide holders or recipients of the information with written declassification instructions. Markings shall be uniformly and conspicuously applied or attached to leave no doubt about the declassified status of the information and who authorized the declassification.

(b) Standard Markings. The following markings shall be applied to declassified records, or copies of records, regardless of media:

(1) The word, "Declassified;"

(2) The authority for the action (e.g., the identity of the OCA who directed the action, or identification of the correspondence or classification instruction that required it);

(3) The date of declassification; and

(4) The overall classification markings that appear on the cover page or first page shall be marked through with an "X" or straight line.

(ISOO Directive No. 1, Section 2001.24)

5. **Reclassification Markings.**

(a) When reclassifying information according to Chapter 2, paragraphs 4 and 5, OCAs must ensure to provide the following markings to holders:

(1) The new overall classification markings;

(2) The new portion markings;

(3) The identity, by name or personal identifier, and position of the OCA;

(4) Declassification instructions;

(5) A concise reason for classification (i.e., the applicable EO 12958, as amended, 1.4 reason); and

(6) The date the action was taken.

(ISOO Directive No. 1, Section 2001.12(d)(1))

CHAPTER 6: SAFEGUARDING

1. **Emergency Authority**.

(a) In emergency situations, in which there is an imminent threat to life or in defense of the homeland, Military Department or other DoD Component Agency Heads or designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

(1) Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose;

(2) Limit the number of individuals who receive it;

(3) Transmit the classified information via approved federal government channels by the most secure and expeditious method according to DoD 5200.1-R, or other means deemed necessary when time is of the essence;

(4) Provide instructions about what specific information is classified, how it should be safeguarded; physical custody of classified information must remain with an authorized federal government entity, in all but the most extraordinary circumstances;

(5) Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement;

(6) Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating Agency of the information and DUSD(CI&S) by providing the following information:

- A description of the disclosed information;
- To whom the information was disclosed;
- How the information was disclosed and transmitted;
- Reason for the emergency release;
- How the information is being safeguarded, and,
- A description of the briefings provided and a copy of the nondisclosure agreements signed.

(EO 12958, as amended, Section. 4.2(b) and ISOO Directive No. 1, Section 2001.51)

APPENDIX 2: DEFINITIONS

Add the following definitions:

Accessioned Records. Records of permanent historical value in the legal custody of NARA.

Authorized Person. A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know for the specific classified information in the performance of official duties.

Declassification Guide. A guide providing classification and declassification instructions specifically for information that is 25 years old or older and of permanent historical value. A declassification guide is also the most commonly used vehicle for obtaining ISCAP approval of 25-year exemptions from the automatic declassification provisions of EO 12958, as amended.

Equity. Information originally classified by or under the control of an Agency.

Exempted. Nomenclature and marking indicating information has been determined to fall within an enumerated exemption from automatic declassification under EO 12958, as amended.

Federal Record. Includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an Agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that Agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference, and stocks of publications and processed documents are not included. (44 USC 3301)

File Series Exemption. An exception to the 25-year automatic declassification provisions of EO 12958, as amended. This exception applies to entire blocks of records, i.e., "file series," within an agency's records management program. To qualify for this exemption, the file series must be replete with exemptible information.

Newly Discovered Records. Records that were inadvertently not reviewed prior to the effective date of automatic declassification because the Agency declassification authority was unaware of their existence.

Pass/Fail (P/F). A declassification technique that regards information at the full document or folder level. Any exemptible portion of a document or folder may result in exemption (failure) of the entire documents or folders. Documents or folders that contain no exemptible information are passed and therefore declassified. Documents within exempt folders are exempt from automatic declassification. Declassified documents may be subject to Freedom of Information Act exemptions other than the security exemption ((b)(1)), and the requirements placed by legal authorities governing Presidential records and materials.

Permanent Records. Any Federal record that has been determined by NARA to have sufficient value to warrant its preservation in the National Archives of the United States. Permanent records include all records accessioned by NARA into the National Archives of the United States and later increments of the same records, and those for which the disposition is permanent on SF 115s, Request for Records Disposition Authority, approved by NARA on or after 14 May 1973.

Presidential Historical Materials and Records. The papers or records of the former Presidents under the legal control of the Archivist pursuant to sections 2107, 2111, 2111note, or 2203 of title 44, USC, as defined at 44 USC 2111, 2111note, and 2001.

Records. The records of an Agency and Presidential papers or Presidential records, as those terms are defined in title 44, USC, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring Agency's control under the terms of the contract, license, certificate, or grant.

Redaction. For purposes of declassification, the removal of exempted information from copies of a document.

Scheduled Records. All records that fall under a NARA approved records control schedule are considered to be scheduled records.

Tab. A narrow paper sleeve placed around a document or group of documents in such a way that it would be readily visible.

Transferred Records. Records transferred to Agency storage facilities or a federal records center.

Temporary Records. Federal records approved by NARA for disposal, either immediately or after a specified retention period. Also called disposable records.

Unscheduled Records. Federal records whose final disposition has not been approved by NARA.

Vault. An area approved by the Agency head, which is designed and constructed of masonry units or steel lined construction to provide protection against forced entry.

INTERIM GUIDANCE
ON
SAFEGUARDING
AND
CONTROLLED UNCLASSIFIED INFORMATION

TABLE OF CONTENTS

Subject	Page
GENERAL	1
CHAPTER 6: SAFEGUARDING	
1. Security Container Labels	1
2. Classified Conferences	1
APPENDIX 3: CONTROLLED UNCLASSIFIED INFORMATION	
1. For Official Use Only (FOUO)	2-4
2. For Official Use Only Law Enforcement Sensitive	5-6
3. Sensitive But Unclassified and Limited Official Use Only	6
4. Limited Distribution Information	6-8

INTERIM GUIDANCE
ON
SAFEGUARDING
AND
CONTROLLED UNCLASSIFIED INFORMATION

GENERAL

The following provides Interim Guidance on changes to the Safeguarding and Controlled Unclassified Information portions of DoD Regulation 5200.1, "Information Security Program," January 1997. It is listed in the order of the chapters in DoD 5200.1-R. References to publications cited throughout this guidance are listed in the reference portion of DoD 5200.1-R. The official change to the regulation will be forthcoming.

CHAPTER 6: SAFEGUARDING

1. **Security Container Labels.** GSA-approved security containers must have a label stating "General Services Administration Approved Security Container," affixed to the front of the container usually on the control or the top drawer. If the label is missing or if the container's integrity is in question, the container shall be inspected by a GSA certified technician. If the container is found to meet specifications, a new label shall be attached. Information on obtaining inspections and recertification of containers can be found on the GSA web page: "http//www.nfc.fss.gsa.gov/security" or on the DoD Lock Program web page: http://locks.nfesc.navy.mil or by calling GSA at (703) 305-7342 or the DoD Lock Program at (800) 290-7607.

2. **Classified Conferences.** In accordance with Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum dated 26 October 2001, Subject: Classified Information at Meetings and Conferences, portions or sessions of meetings, conferences, etc., during which classified information is to be disseminated shall be limited to appropriately cleared U.S. Government or U.S. Government contractor locations.

APPENDIX 3: CONTROLLED UNCLASSIFIED INFORMATION

1. FOR OFFICIAL USE ONLY (FOUO).

(a) General. Information that is currently and properly classified shall be withheld from mandatory release under the first exemption of the Freedom of Information Act FOIA (reference (l)). "FOR OFFICIAL USE ONLY" (FOUO) is applied to information that may be exempt under one or more of the other eight exemptions. So, by definition, information shall be unclassified in order to be designated FOUO. If an item of classified information is declassified, it may be designated FOUO if it qualifies under one of the other exemptions of the FOIA (reference (l)). This means that:

(1) Information cannot be classified and FOUO at the same time. Therefore, classified documents containing FOUO information cannot bear an overall document marking of FOUO. However, portions or pages of a classified document, that contain only FOUO information will be marked as FOUO.

(2) Information that is declassified may be designated FOUO, only if it is believed to fit into one or more of the last eight exemptions (exemptions 2 through 9).

(b) Marking.

(1) Marking information FOUO does not automatically qualify it for exemption. If a request for a record is received, the information shall be reviewed to determine if it actually qualifies for exemption. Similarly, the absence of the FOUO marking does not automatically mean the information shall be released. Some types of records (for example, personnel records) are not normally marked FOUO, but may still be withheld under the FOIA (reference (l)). All DoD unclassified information must be reviewed before it is released to the public or to foreign governments and international organizations.

(2) Portion Marking FOUO Information. Subjects, titles and each section, part, paragraph, and similar portion of an FOUO document shall be marked to show that they contain information requiring protection. Use the

parenthetical notation "(FOUO)" to identify information as For Official Use Only for this purpose. Place this notation immediately before the text.

(c) Access to FOUO Information.

(1) No person may have access to information designated as FOUO unless that person has been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose.

(2) The final responsibility for determining whether an individual has a valid need for access to information designated as FOUO rests with the individual who has authorized possession, knowledge or control of the information and not on the prospective recipient.

(3) Information designated as FOUO may be disseminated within the DoD Components and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct official business for the Department of Defense, provided that dissemination is not further controlled by a Distribution Statement.

(4) DoD holders of information designated as FOUO are authorized to convey such information to officials in other Departments and Agencies of the Executive and Judicial Branches to fulfill a government function. If the information is covered by the Privacy Act (reference (o)), disclosure is only authorized if the requirements of DoD 5400.11-R (reference (s)) are satisfied.

(5) Release of FOUO information to Congress is governed by DoD Directive 5400.4 (reference (t)). If the information is covered by the Privacy Act (reference (o)), disclosure is authorized if the requirements of DoD 5400.11-R (reference (s)) are also satisfied.

(6) DoD Directive 7650.1 (reference (u)) governs release of FOUO information to the General Accounting Office (GAO). If the information is covered by the Privacy Act (reference (o)), disclosure is authorized if the requirements of DoD 5400.11-R (reference (u)) are also satisfied.

(d) Protection of FOUO Information

(1) During working hours, reasonable steps shall be taken to minimize risk of access by unauthorized personnel. After working hours, store FOUO information in unlocked containers, desks or cabinets if Government or Government-contract building security is provided. If such building security is not provided, store the information in locked desks, file cabinets, bookcases, locked rooms, etc.

(2) FOUO information and material may be transmitted via first class mail, parcel post or, for bulk shipments, via fourth class mail. Electronic transmission of FOUO information, e.g., voice, data or facsimile, e-mail, shall be by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI), whenever practical.

(3) FOUO information may only be posted to DoD Web sites consistent with security and access requirements specified in Deputy Secretary of Defense Memorandum dated December 1998, Subject: "Web Site Administration" (reference (v)).

(4) Record copies of FOUO documents shall be disposed of according to the Federal Records Act (reference (w)) and the DoD Component records management directives. Non-record FOUO documents may be destroyed by any of the means approved for the destruction of classified information, or by any other means that would make it difficult to recognize or reconstruct the information.

(e) Unauthorized Disclosure. The unauthorized disclosure of FOUO does not constitute an unauthorized disclosure of DoD information classified for security purposes. However, appropriate administrative action shall be taken to fix responsibility for unauthorized disclosure of FOUO whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act (reference (o)) may also result in civil and criminal sanctions against responsible persons. The Military Department or other DoD Component that originated the FOUO information shall be informed of its unauthorized disclosure.

2. FOR OFFICIAL USE ONLY Law Enforcement Sensitive

(a) Description. Law Enforcement Sensitive is a marking sometimes applied, in addition to/conjunction with the marking FOR OFFICIAL USE ONLY, by the Department of Justice and other activities in the law enforcement community. It is intended to denote that the information was compiled for law enforcement purposes and should be afforded appropriate security in order to protect certain legitimate government interests, including the protection of: enforcement proceedings; the right of a person to a fair trial or an impartial adjudication; grand jury information; personal privacy including records about individuals requiring protection under the Privacy Act (reference (o)); the identity of a confidential source, including a State, Local, or foreign agency or authority or any private institution which furnished information on a confidential basis; information furnished by a confidential source; proprietary information; techniques and procedures for law enforcement investigations or prosecutions; guidelines for law enforcement investigations when disclosure of such guidelines could reasonably be expected to risk circumvention of the law, or jeopardize the life or physical safety of any individual, including the lives and safety of law enforcement personnel.

(b) Markings.

(1) In unclassified documents containing Law Enforcement Sensitive information, the words "Law Enforcement Sensitive" shall accompany the words "FOR OFFICIAL USE ONLY" at the top and bottom of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one).

(2) In unclassified documents, each page containing FOR OFFICIAL USE ONLY Law Enforcement Sensitive information shall be marked "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" at the top and bottom. Classified documents containing such information shall be marked as required by Chapter 5, DoD 5200.1-R except that pages containing Law Enforcement Sensitive information but no classified information will be marked "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" top and bottom.

(c) Portions of DoD classified or unclassified documents that contain FOR OFFICIAL USE ONLY Law Enforcement Sensitive information shall be marked "(FOUO-LES)" at the beginning of the portion. If a portion of a classified document contains both classified and FOR OFFICIAL USE ONLY Law Enforcement Sensitive information, the appropriate classification designation is sufficient to protect the information.

(d) Access to FOR OFFICIAL USE ONLY Law Enforcement Sensitive. The criteria for allowing access to FOR OFFICIAL USE ONLY Law Enforcement Sensitive are the same as those used for FOUO information.

(e) Protection of FOR OFFICIAL USE ONLY Law Enforcement Sensitive. Within the Department of Defense, FOR OFFICIAL USE ONLY Law Enforcement Sensitive shall be protected as required for FOUO information.

3. **Sensitive But Unclassified and Limited Official Use Only**

(a) Access. Within the Department of Defense, the criteria for allowing access to SBU information are the same as those used for FOUO information, except that information received from the Department of State marked SBU shall not be provided to any person who is not a U.S. citizen without the approval of the Department of State activity that originated the information.

4. **LIMITED DISTRIBUTION Information**

(a) Description. LIMITED DISTRIBUTION is a caveat used by the National Geospatial-Intelligence Agency (NGA) to identify a select group of sensitive but unclassified imagery or geospatial information and data created or distributed by NGA or information, data, and products derived from such information. DoD Directive 5030.59 (reference (aa)) contains details of policies and procedures regarding use of the LIMITED DISTRIBUTION caveat. These policies and procedures are summarized below.

(b) Marking. Information or material designated as LIMITED DISTRIBUTION, or derived from such information or material shall, unless otherwise approved by the Director, NGA, be marked as follows:

LIMITED DISTRIBUTION Notation

UNCLASSIFIED/LIMITED DISTRIBUTION Distribution authorized to DoD, IAW 10 U.S.C. §§ 130 and 455. Release authorized to U.S. DoD Contractors IAW 48 C.F.R. §252.245-7000. Refer other requests to Headquarters, NGA, ATTN: Release Officer, Stop D-136. Destroy as "For Official Use Only." Removal of this caveat is prohibited.

(c) Access to LIMITED DISTRIBUTION Information or Material

(1) Information bearing the LIMITED DISTRIBUTION caveat shall be disseminated by NGA to Military Departments or other DoD Components, and to authorized grantees for the conduct of official DoD business.

(2) DoD civilian, military and contractor personnel of a recipient DoD Component, contractor or grantee may be granted access to information bearing the LIMITED DISTRIBUTION caveat provided they have been determined to have a valid need to know for such information in connection with the accomplishment of official business for the Department of Defense. Recipients shall be made aware of the status of such information, and transmission shall be by means to preclude unauthorized disclosure or release. Further dissemination of information bearing the LIMITED DISTRIBUTION caveat by receiving contractors or grantees to another Military Department, other DoD Component, contractor or grantee, or dissemination by any recipient Component, contractor, or grantee to any person, agency or activity outside DoD, requires the express written approval of the Director, NGA.

(3) Information bearing the LIMITED DISTRIBUTION caveat, or derivative information, shall not be released, made accessible to or sold to foreign governments or international organizations, to include through Foreign Security Assistance transactions or arrangements, or transfer or loan of any weapon or weapon system that uses such information, or intended to

be used in mission planning systems, or through the Foreign Military Sales process, without the express, written approval of the Director, NGA.

(4) All Freedom of Information Act requests for information bearing the LIMITED DISTRIBUTION caveat or derived therefrom, shall be referred to NGA consistent with DoD Directive 5030.59 (reference (aa)).

(d) Protection of LIMITED DISTRIBUTION Information.

(1) Information bearing the LIMITED DISTRIBUTION caveat, or derivative information, shall not be stored on systems accessible by contractors, individuals who are not directly working on a DoD contract, or those who do not require access to such information in connection with the conduct of official Department of Defense business.

(2) LIMITED DISTRIBUTION information or derivative information, may only be posted to DoD Web sites consistent with security and access requirements specified in Deputy Secretary of Defense Memorandum dated December 1998 (reference (v)). Such information shall not be transmitted over the World Wide Web or over other publicly accessible and unsecured systems. Electronic transmission of such information, e.g., voice, data or facsimile, shall be by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure.

(3) Store LIMITED DISTRIBUTION information in the same manner approved for FOUO.

(4) When no longer required, all LIMITED DISTRIBUTION information and copies, shall be returned to NGA or destroyed in a manner sufficient to prevent its reconstruction.