



2010 DTIC CONFERENCE
March 22-24, 2010

Celebrating 65 Years of Providing Access to Defense Information

Developments in Information Security Management

22 March 2010

Mr. Robert A. Van Veghel, Moderator



Developments in Information Security Management

DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004

Developments in Information Security Management:

- Executive Order 13526 "Classified National Security Information"
- Plans for National Declassification Center
- Status of Controlled Unclassified Information



Developments in Information Security Management

DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004

Mr. William A. Cira

Associate Director, Classification Management
National Archives and Records Administration (NARA)
Information Security Oversight Office

Ms. Carroll Lee

DoD CUI Policy
Office of the Under Secretary of Defense (Intelligence)



Developments in Information Security Management

DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004

Ms. Deborah Ross

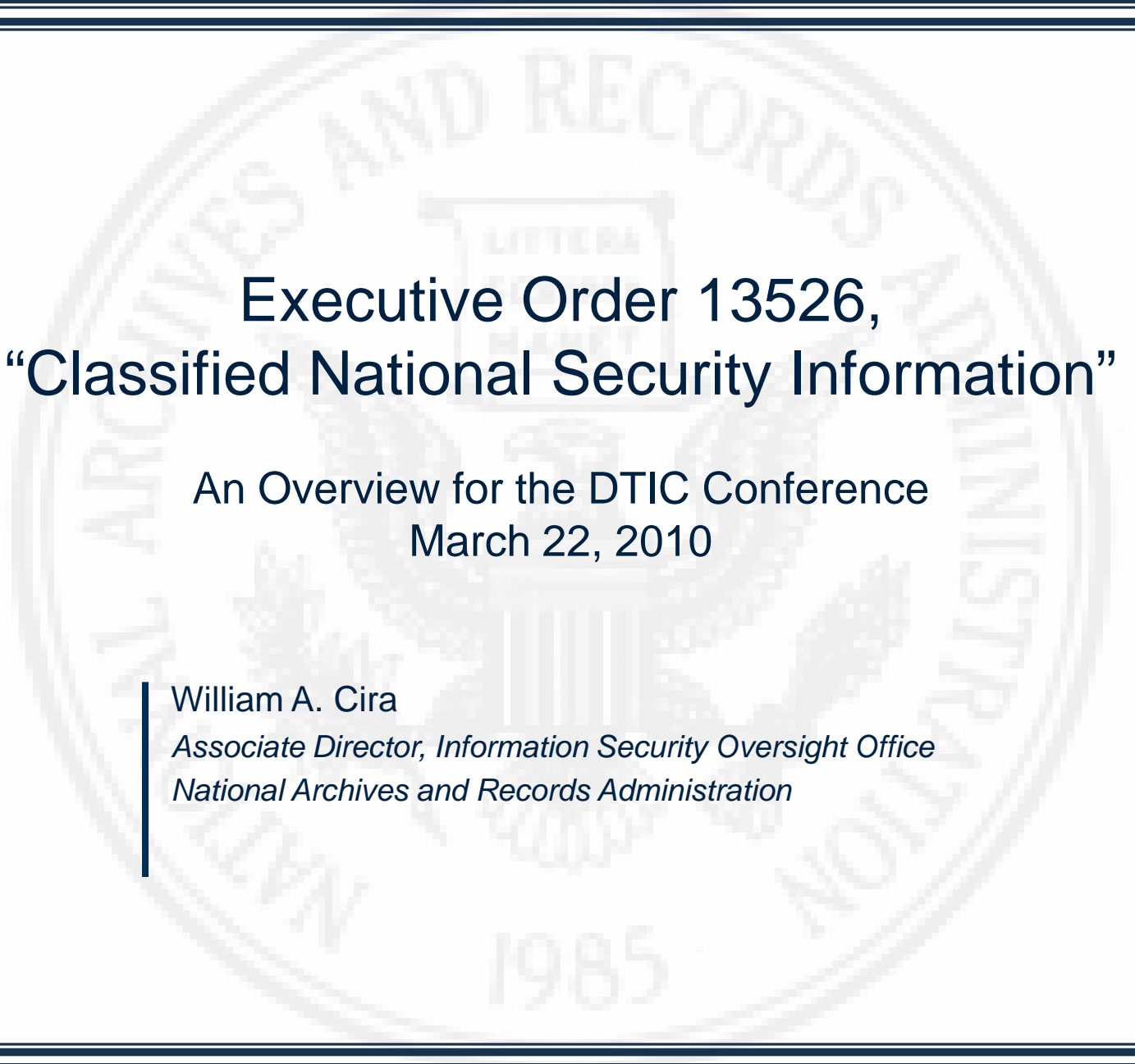
DoD Information Security Policy

Office of the Under Secretary of Defense (HUMINT,
Counterintelligence and Security)

Mr. Ed Kaufhold

DoD Declassification Policy

Office of the Under Secretary of Defense (Intelligence)



Executive Order 13526, “Classified National Security Information”

An Overview for the DTIC Conference
March 22, 2010

William A. Cira

*Associate Director, Information Security Oversight Office
National Archives and Records Administration*



Presidential Actions of December 29, 2009

- Executive Order 13526, “Classified National Security Information”
- Presidential Memorandum, Implementation of the Executive Order, “Classified National Security Information”
- Administrative Order, “Original Classification Authority”

Establishes a uniform system for classifying, safeguarding, and declassifying national security information.

Promotes the President’s agenda of greater openness and transparency while enhancing national security.



E.O. 13526 & National Declassification Center

Section 3.7

- Collaborative declassification review, under the administration of a Director appointed by the Archivist in consultation with his counterparts at the major national security departments.
- General functions of the Center shall apply to all archival records, regardless of whether they have yet been accessioned into NARA, and all referral processing of accessioned records shall take place under the direction of the Center.
- Agencies will review archival records in accordance with priorities developed by the Archivist, with input from the general public, that take into account the level of researcher interest and the likelihood of declassification.



E.O. 13526 & Over-Classification

- No information may remain classified indefinitely. **Section 1.5(d)**
- Emphasizes the requirement to identify describable damage to the national security before classifying information. **Section 1.4**
- Restores the presumption against classification and in favor of a lower level of classification in cases of “significant doubt.” **Sections 1.1(b) and 1.2(c)**
- Requires agencies to conduct fundamental classification guidance reviews to ensure that classification guides reflect current conditions. An unclassified version of a report on such reviews shall be made public by each agency. **Section 1.9**



E.O. 13526 & Over-Classification (continued)

- Tightens the standards for keeping information classified for more than 25 years. **Sections 3.3(b) and 3.3(h)**
- Greatly strengthens requirements for the training of all OCAs and the much larger number of derivative classifiers. **Sections 1.3(d) and 2.1(d)**
- Adds a requirement to identify derivative classifiers by name and position, or by personal identifier on each document they derivatively classify. **Section 2.1(b)(1)**



E.O. 13526 & Over-Classification (continued)

- Mandates that agency self-inspection programs shall review original and derivative classification decisions and correct misclassification actions appropriately. **Section 5.4(d)(4)**
- Directs agency heads to establish an internal, secure capability to receive complaints regarding over-classification and to provide guidance to personnel. **Section 5.4(d)(10)**



E.O. 13526 & Information Sharing

- Revises the Preamble to emphasize “the responsibility to provide information both within the government and to the American people.”
- Calls for maximum possible access to classified information by persons who meet standard criteria for access. **Section 4.2(a)**
- Calls for the greatest practicable use of standardized electronic protocols and formats in order to maximize the accessibility and safeguarding of classified electronic information. **Section 4.1(f)**



E.O. 13526 & Information Sharing (continued)

- Modifies the “third agency rule” to authorize re-dissemination of classified materials by third agencies, except in limited exceptional cases, without the approval of the originating agency. **Section 4.1(i)**
- Revises the definition of “need-to-know” to shift the focus to prospective recipients with a mission need for information rather than a determination made by “owners” of the information. **Section 6.2(dd)**
- Mandates the use of classified addendums or unclassified versions of documents whenever possible to facilitate greater information sharing. **Sections 1.6(g) and 2.1(c)**



E.O. 13526 & Reclassification

- Prohibits the reclassification of information after its declassification and release under proper authority except when agencies can comply with significantly tightened restrictions, particularly regarding records that have been accessioned into the National Archives. **Section 1.7(c)**



E.O. 13526 & “Other Measures”

- Eliminates the Intelligence Community veto of declassification decisions made by the Interagency Security Classification Appeals Panel (ISCAP) regarding intelligence sources and methods. **Section 5.3(f)**
- Strengthens the standards that agencies must meet to exempt any records from automatic declassification at 25 years. **Section 3.3(h)**
- Identifies with greater specificity information that can be exempted from automatic declassification because it relates to intelligence sources and methods or military war plans. **Section 3.3(b)**



E.O. 13526 & “Other Measures” (continued)

- Requires specific deadlines for the declassification of information exempted from automatic declassification at 25 years and prohibits classification beyond 75 years except in extraordinary cases and as approved by ISCAP. **Section 3.3(h)**
- Directs that the review of third agency referrals subject to automatic declassification shall be performed in a prioritized manner determined by the NDC rather than according to a rigid schedule. **Sections 3.3(d)(3), 3.7(b)(1), and 3.7(d)**
- Directs agencies to consider final decisions of the ISCAP when making declassification decisions. **Section 3.1(i)**



E.O. 13526 & “Other Measures” (continued)

- Provides guidance for the first time regarding the declassification of non-archival and non-record material. **Section 3.1(h)**
- Limits the time span of records that may be included in a single integral file block for declassification purposes. **Section 6.1(v)**
- Provides that no information may be excluded from automatic declassification based solely on the physical type of the document/record in which it is found. **Section 3.1(g)**
- Requires a review of previously approved file series exemptions. **Section 3.3(c)(4)**



Important Dates

- **December 29, 2009**
 - Sections 1.7, 3.3, and 3.7 of E.O. 13526 were effective.
- **April 28, 2010**
 - Agency reports on delegations of OCA are due.
- **June 27, 2010**
 - All remaining sections of E.O. 13526 are effective.
- **December 2011 (no later than)**
 - Agency regulations issued in final form.
 - 180 days from issuance of 32 C.F.R. Part 2001 by ISOO.
- **December 31, 2013**
 - Backlog to be completed by NDC.



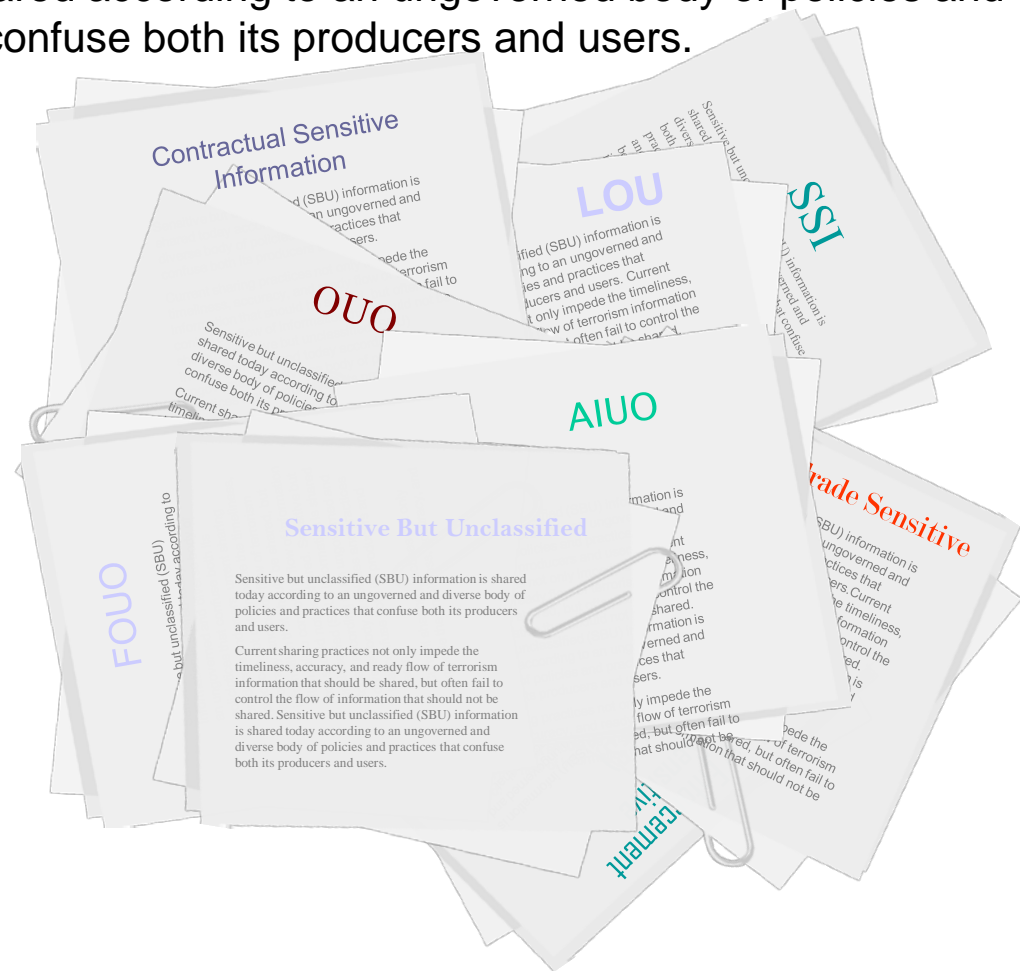
SBU Information

SBU information is currently shared according to an un governed body of policies and practices that confuse both its producers and users.

Inconsistency in SBU policies greatly increases the **likelihood of erroneous handling and sharing** of information.

Across the Federal government there are at least **107 unique markings** and over **130 different labeling or handling processes** and procedures for SBU information.

Current SBU sharing practices not only **impede the timeliness, accuracy, and ready flow** of information that should be shared, but often **fail to protect information** in a consistent and transparent manner.





Presidential Memorandum, May 9, 2008: *The Designation and Sharing of Controlled Unclassified Information*

This Memorandum:

- Adopts, defines, and institutes “Controlled Unclassified Information” (CUI) as the single categorical designation for all information referred to as “Sensitive But Unclassified” (SBU) in the Information Sharing Environment (ISE); and
- Establishes a corresponding new CUI Framework for designating, marking, safeguarding, and disseminating information designated as CUI; and
- Designates the National Archives and Records Administration (NARA) as the Executive Agent, to oversee and implement the new CUI Framework.



For Immediate Release
Office of the Press Secretary
May 9, 2008

Memorandum For The Heads Of Executive Departments And Agencies

SUBJECT: Designation and Sharing of Controlled Unclassified Information (CUI)

PURPOSE

(1) This memorandum (a) adopts, defines, and institutes “Controlled Unclassified Information” (CUI) as the single, categorical designation henceforth throughout the executive branch for all information within the scope of that definition, which includes most information heretofore referred to as “Sensitive But Unclassified” (SBU) in the Information Sharing Environment (ISE), and (b) establishes a corresponding new CUI Framework for designating, marking, safeguarding, and disseminating information designated as CUI. The memorandum’s purpose is to standardize practices and thereby improve the sharing of information, not to classify or declassify new or additional information.

Background – The Current SBU Environment

(2) The global nature of the threats facing the United States requires that (a) our Nation’s entire network of defenders be able to share information more rapidly so those who must act have the information they need, and (b) the United States Government protect sensitive information, information privacy, and other legal rights of Americans. A uniform and more standardized governmentwide framework for what has previously been known as SBU information is essential for the ISE to succeed. Accordingly, this memorandum establishes a standardized framework designed to facilitate and enhance the sharing of Controlled Unclassified Information.

Definitions

(3) In this memorandum, the following terms have the meaning indicated:

a. “Controlled Unclassified Information” is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces “Sensitive But Unclassified” (SBU).

b. “CUI Council” is a subcommittee of the Information Sharing Council (ISC), created by the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458) (IRTPA).

c. “CUI Framework” refers to the single set of policies and procedures governing the designation, marking, safeguarding, and dissemination of CUI terrorism-related information that originates in departments and agencies, regardless of the medium used for the display, storage, or transmittal of such information.

1

The purpose of the CUI Framework is to standardize practices and thereby improve the sharing of information.



Presidential Memorandum, May 27, 2009 *Controlled Unclassified Information*

Created Task Force jointly headed by DHS and DOJ, charged with:

- reviewing current procedures for categorizing and sharing SBU; and
- making recommendations within 90 days regarding how the executive branch should proceed with respect to the CUI Framework.
 - Scope (terrorism-related within the ISE or all SBU/CUI).
 - Measurement of agency progress.
- “Recommendations shall recognize and reflect a balancing of the following:
 - “a presumption in favor of openness in accordance with the President’s memoranda of January 21, 2009 on Transparency and Open Government and on FOIA;”
 - “the value of standardizing the procedures for designating, marking, and handling all SBU information; and”
 - “the need to prevent the public disclosure of information where such disclosure would compromise privacy or other legitimate interests.”



Task Force Report to the President

- Signed by Attorney General and Secretary of DHS
- Submitted to the White House
- Accepted by the President and released to the public
 - http://www.dhs.gov/ynews/releases/pr_1260887995817.shtm
- Ongoing CUI reform effort led by the White House and involving all major CUI stakeholders



Resources

- Executive Order 13526, “Classified National Security Information”
 - <http://www.archives.gov/isoo/pdf/cnsi-eo.pdf>
- Presidential Memorandum, Implementation of the Executive Order, “Classified National Security Information”
 - <http://www.archives.gov/isoo/pdf/implementing-memo.pdf>
- Administrative Order, “Original Classification Authority”
 - <http://www.archives.gov/isoo/pdf/oca.pdf>



Contact Information

Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, N.W., Room 100
Washington, DC 20408-0001

(202) 357-5250 (voice)

(202) 357-5907 (fax)

isoo@nara.gov (email)

www.archives.gov/ISOO (website)



DOD INFORMATION SECURITY POLICY

Deborah Ross
Information Security Policy
Office of the Under Secretary of Defense (Intelligence)

March 2010

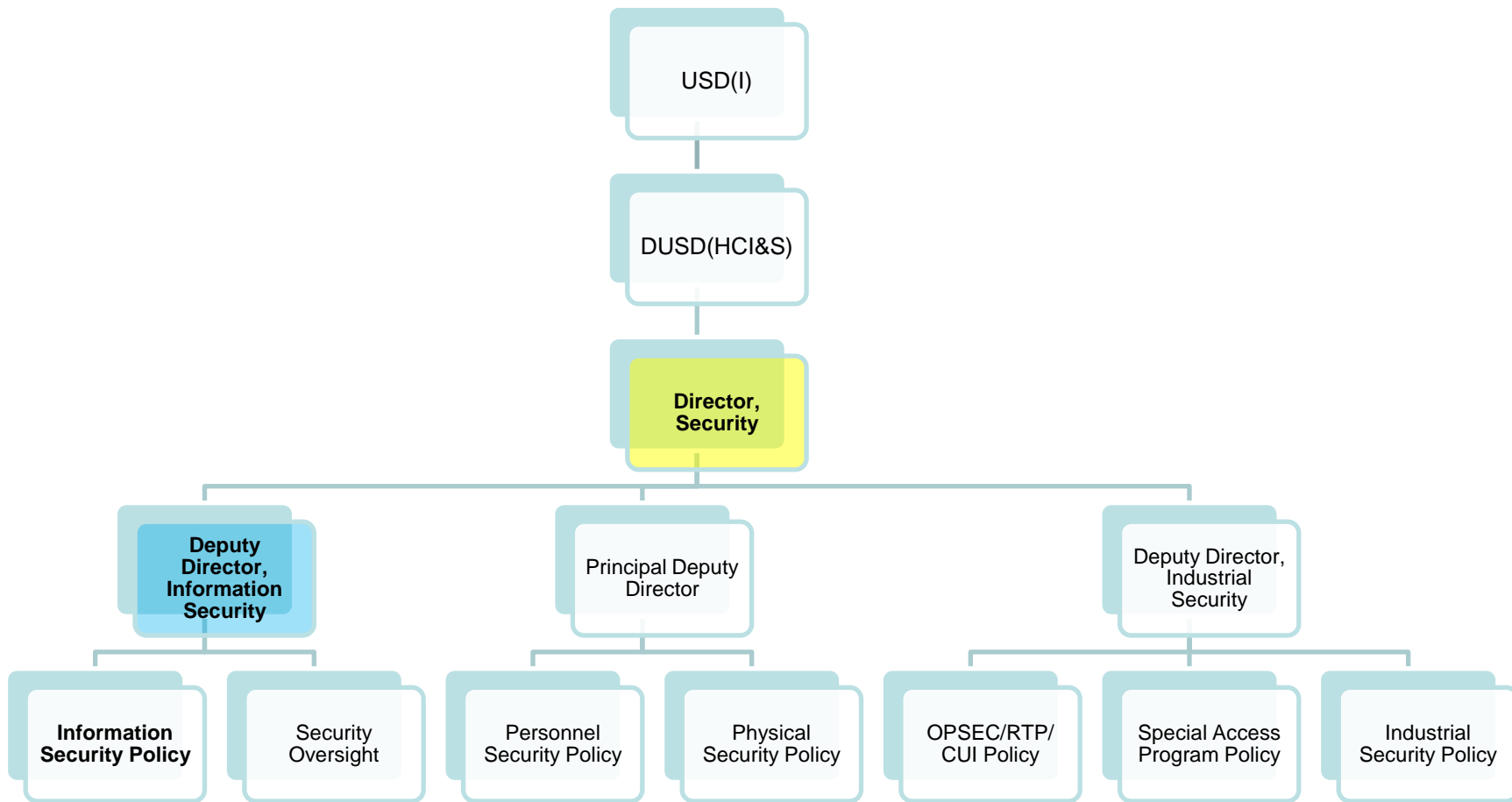


Overview

- Organization
- Responsibilities
- Policy
- Implementation Plans



Organization





Responsibilities

- Policy
- Oversight



Policy

- DoDI 5200.01 – DoD Information Security Program and Protection of Sensitive Compartmented Information
- DoD 5200.1-R – Information Security Program Regulation
- DoD 5200.1-R Supplemental Policy
 - DTM 04-010 – Interim Information Security Guidance



Policy

- DoD 5200.1-R Supplemental Policy
 - DTM 07-021 – Declassification Marking Guidance for DoD Special Access Program (SAP) Classified Material
 - DTM 05-008 – Use of the "Not Releasable to Foreign Nationals" (NOFORN) Caveat on Department of Defense (DoD) Information
 - DTM 04-009 – Security Classification Marking Instructions



Implementation Plans

- DTM
 - Implements immediate provisions of EO 13526
 - Temporary measure
 - Implements 3 sections of EO
 - 1.7 (Prohibitions & Limitations)
 - 3.3 (Automatic Declassification)
 - 3.7 (National Declassification Center)



Implementation Plans

- Impacts 3 issuances
 - DoDI 5200.01
 - DoD 5200.1-R
 - DTM 04-010 Updated in draft DoD 5200.1-R revision

- Status: Entered into DoD issuance coordination process



Implementation Plans

- Update to DoD 5200.1-R
 - Converted to a Manual w/4 Volumes (DoDM 5200.01)
 - Volume I (Program Management, Classification, Declassification)
 - Volume II (Marking)
 - Volume III (Safeguarding)
 - Volume IV (CUI)
 - Includes all EO 13526 provisions



Implementation Plans

- Status: Entered into DoD issuance coordination process
- Continue to participate in national-level policy development
 - Now revising ISOO Directive No. 1
 - Our office represents DoD



The National Declassification Center and DoD's Joint Referral Center

Ed Kaufhold
Security Specialist, Information Security Policy
Office of the Under Secretary of Defense (Intelligence)

22 March, 2010



Agenda

- **National Declassification Center (NDC)**
 - Overview and Background
 - The “Backlog”
 - The NDC BPR
 - NDC Related Initiatives
- **DoD Joint Referral Center (JRC)**
 - JRC Overview and Background
 - JRC Concept of Operations
 - JRC and NDC Interfaces
- **Questions**



NDC Overview and Background

- **Established by E.O. 13526, Section 3.7**
 - “There is established within the National Archives a National Declassification Center to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value...”
- **Additional guidance in POTUS memo, 29 DEC 09:**
 - Under the direction of the National Declassification Center (NDC)...referrals and quality assurance problems within a backlog of more than 400 million pages ... shall be addressed in a manner that will permit public access to **all** declassified records from this backlog no later than December 31, 2013.
- **Currently located at NARA, Archives II, College Park, MD**



NDC Overview and Background

- Under the administration of the Director, the Center shall coordinate:
 - (1) **timely and appropriate processing of referrals** ... for accessioned Federal records and transferred presidential records;
 - (2) **general interagency declassification activities** necessary to fulfill the requirements of ... this order;
 - (3) **the exchange among agencies of detailed declassification guidance** to enable the referral of records in accordance with ...this order;
 - (4) the **development of effective, transparent, and standard declassification work processes, training, and quality assurance measures;**
 - (5) the **development of solutions to declassification challenges posed by electronic records, special media, and emerging technologies;**
 - (6) the **linkage and effective utilization of existing agency databases and the use of new technologies** to document and make public declassification review decisions and support declassification activities under the purview of the Center; and
 - (7) storage and related services, on a reimbursable basis, for Federal records containing classified national security information.



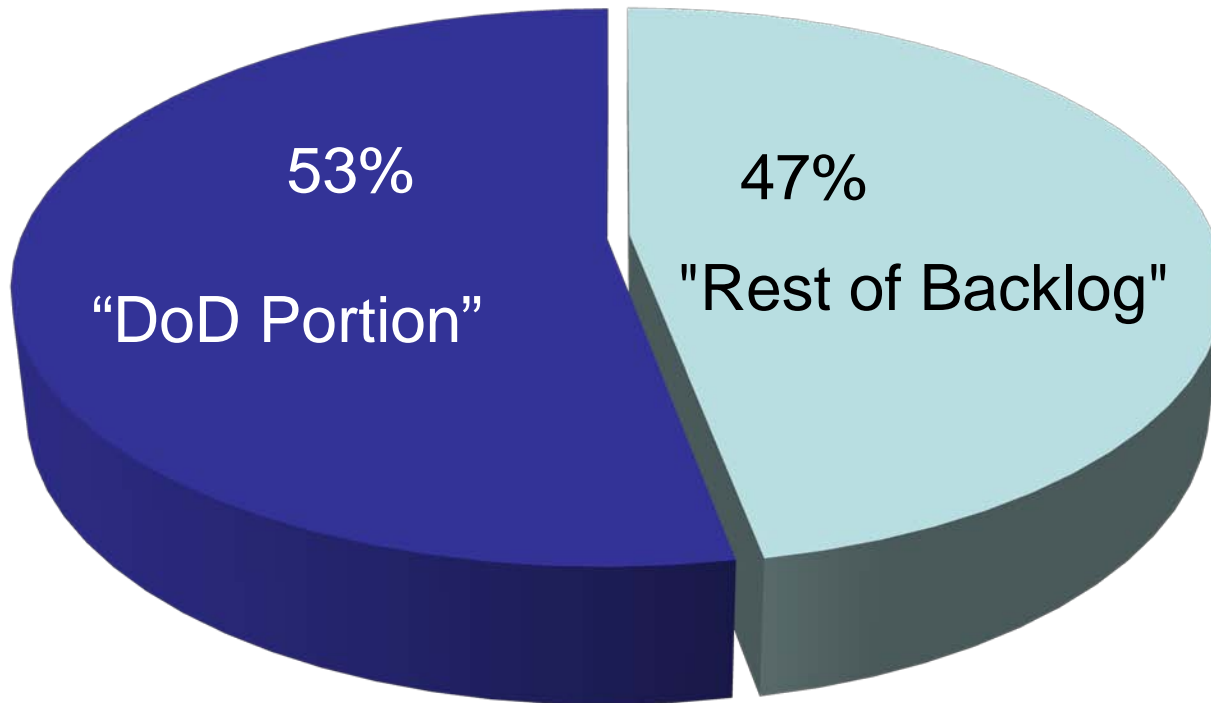
“The Backlog”

- **What is it?**
 - Permanently valuable Federal records that are in the legal custody of NARA, as required by in Title 44, US Code;
 - Estimated to total 408M pages, stored in 160,000 - 240,000 (variously sized) boxes;
 - DoD components previously reviewed (declassified or exempted) all of their material to meet established Presidentially mandated (E.O. 12958) deadlines;
 - NARA will prioritize the Backlog retirement review process in order to accommodate interests of researchers and public interest groups;
 - Growing by ~ 4 M pages per year (all sources)



“The Backlog”

■ Rest of Backlog: 192 M ■ DoD Portion: 216 M



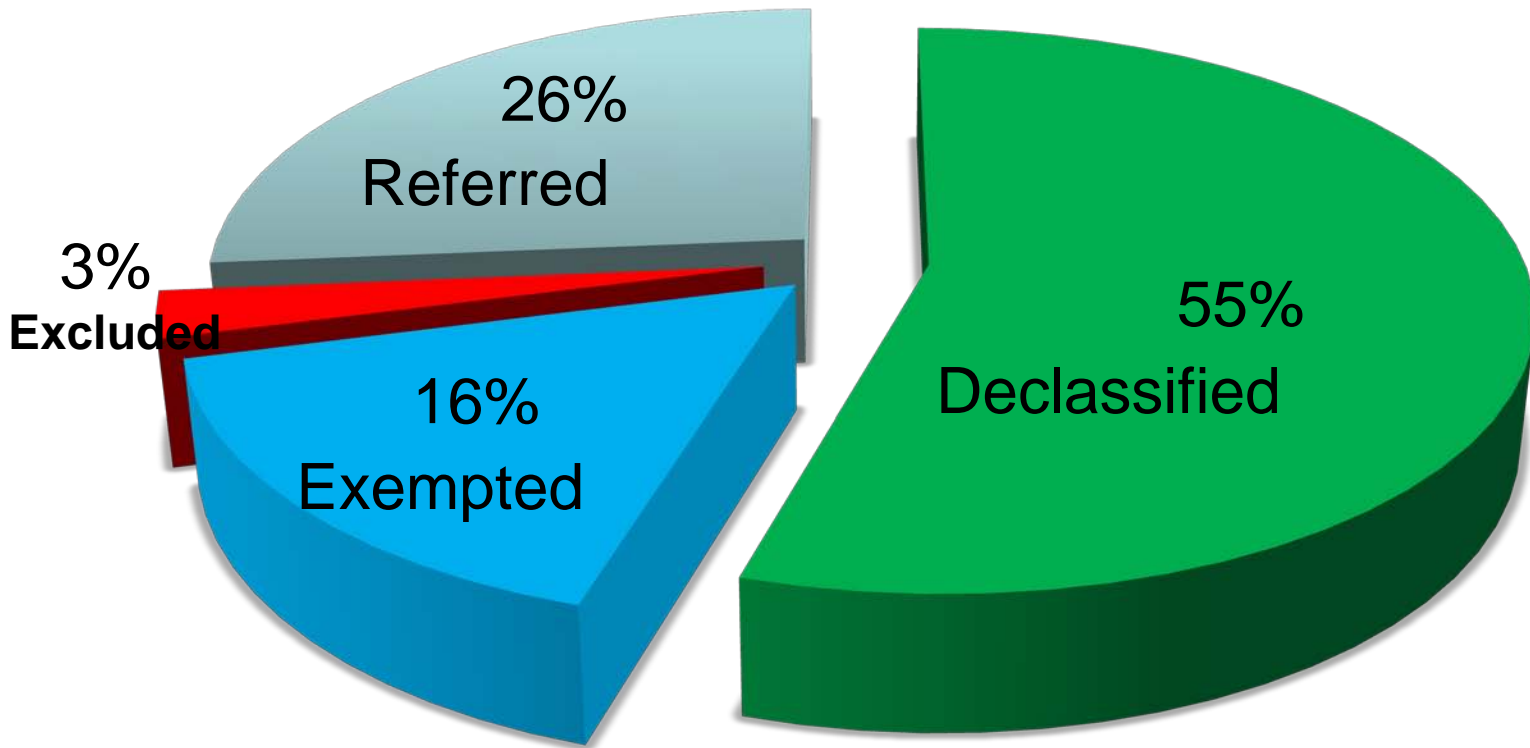
Source:

MAR 2010 Analysis of DoD Information--Consolidated Army, Navy, Air Force, Joint Staff and OSD Portion of the 408 M Backlog, 1996 -- 2009



“The Backlog”

■ Declassified ■ Exempted ■ Excluded ■ Referred



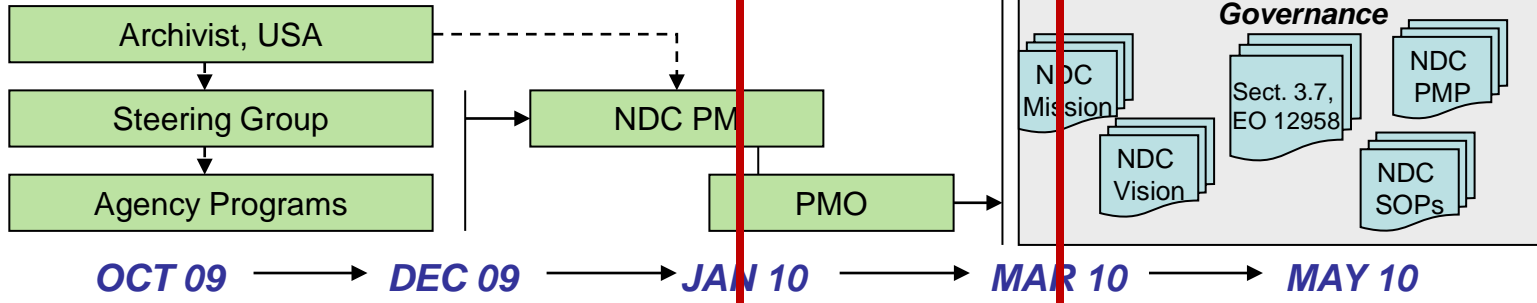
Source:

MAR 2010 Analysis of DoD Information--Consolidated Army, Navy, Air Force, Joint Staff and OSD Portion of the 408 M Backlog, 1996 – 2009



The NDC BPR

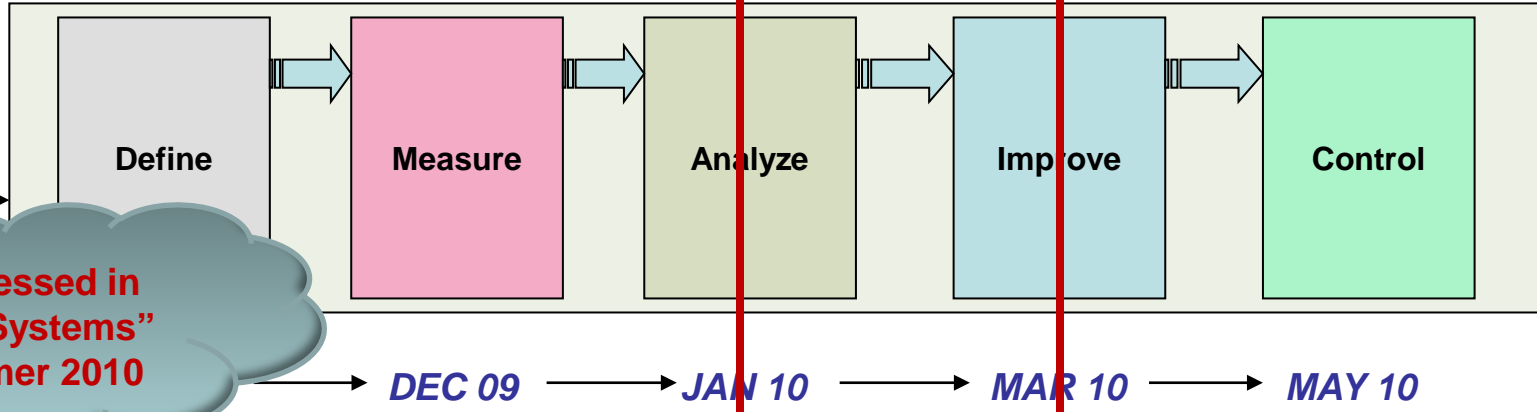
People



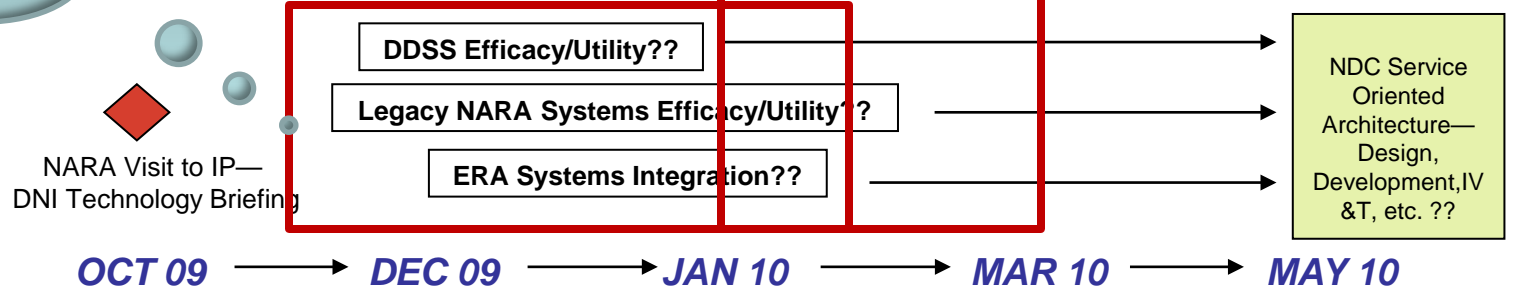
Process

Cross Funx

To be addressed in follow-on "Systems" BPR, Summer 2010



Technology





NDC Related Initiatives

- **DoD Manpower Study**
 - Currently, ~ 370 [Non-NARA] USG and Contractor FTEs executing Automatic Declassification programs;
 - The NDC must “retire” ~ 500,000 pages per day in the next 40 months;
 - Application of solid, analytically-based risk management and manpower planning is going to be essential.
- **We are now engaged with MILDEP and OSD planning elements to organize a DoD-team manpower requirements study...**



JRC Overview and Background

- Established by Loan Agreement between NARA and OUSD(I), memo finalized 26 JAN 10. Details:
 - Eligible [accessioned] records to be loaned from NARA may include:
 - All classified DoD Record Groups that contain permanent, historical records that are 25 years or older.
 - Records stored at National Archives facilities.
 - Records that do not require special handling or storage conditions due to their fragile condition, or are otherwise deteriorated to the extent that further handling will endanger them.
 - Records that are not of high intrinsic value.
 - Records that are not needed for immediate and critical research uses by the Federal government and/or the general public.
- An 18-month, OUSD(I)-sponsored Pilot activity.
- Currently co-located with the Army Declassification Activity near Ft. Belvoir, VA.



JRC Concept of Operations

- Guided by a multi-DoD Component Charter signed 19 JAN 10:
 - **Crawl – Walk – Run !**
 - MILDEPs, Joint Staff, OSD/WHS, and NRO are “plank-owners;”
 - DIA, MDA, NGA, NSA aligning to engage;
 - NARA personnel on-site;
 - Overarching goal: clear all DoD referrals and return a finished product to NARA
- Operational schedule thru IOC:
 - **Week 1 (8-12 Mar 10)**
 - Ribbon Cutting and Component equities training
 - **Week 2 - (15-19 Mar 10)**
 - Systems orientation; workflow familiarization;
 - JRC reviews commence & IOC declaration



JRC and NDC Interfaces

- Section 3.7(e) of EO 13526 directs that, "...Once [the NDC] is established, all referral processing of accessioned records shall take place [at the NDC]."
 - No conflict. The NDC "to-be" business processes will not be crystallized until at least late-May, 2010, when the ongoing BPR will enter Control-phase analysis.
 - Full NDC IOC -- TBD
 - Meanwhile, the JRC is organized and operational today, to begin making progress on the DoD's existing referrals within the NDC Backlog
 - While simultaneously serving as a test-bed for to-be NDC processes, information systems and technology integration, and training.



Controlled Unclassified Information (CUI)

Carroll S. Lee
DoD Controlled Unclassified Information Policy
Office of the Under Secretary of Defense (Intelligence)

22 March 2010



CUI Framework

- May 27, 2009 Presidential memorandum
 - Reaffirmed White House mandate of May 2008 to:
 - Streamline 107 federal dissemination and safeguarding markings into 3 basic markings
 - Focus on information related to counter-terrorism, weapons of mass destruction and law enforcement
 - Establish the National Archives and Records Administration as Executive Agent



CUI Framework

- May 27, 2009 Presidential memorandum
 - Created an interagency Task Force to review current and proposed policy and procedures
 - Task Force report completed in August 2009
 - Contained 40 recommendations
 - Task Force report accepted by White House in December 2009
 - Report is located on the DHS website
 - www.dhs.gov/xlibrary/assets/cui_task_force_rpt.pdf - 2009-12-15



Task Force Recommendations

- That an Executive Order for CUI be written
- Expanding scope to encompass all sensitive unclassified information
- Accelerating timeline to complete all implementation by May 2013
- Decontrol of CUI material after 10 years
- Single Federal Acquisition Regulation clause for protection of CUI in industry



Challenges

- Implementing new requirements
- Establishment of a process to decontrol CUI material
- Ensure training reaches 100% of DoD personnel and affected DoD contractors
- Training tailored to specific areas of responsibility
- Modify DoD policies to reflect new CUI Framework



New for DoD

As conceived in the Task Force Report:

- Requirement for new markings for CUI materials
- DoD CUI designations reported to and approved by the CUI EA
- DoD CUI implementing regulations reviewed by EA prior to issuance
- Remarking of legacy materials placed back in circulation
- Upgrade IT systems using new CUI markings



DoD Planning Action

- DoD CUI Implementation Activity initiated in December 2007
- Draft DoD CUI Transition and Strategic Plan issued in May 2009 and updated in December 2009
- Initialized efforts to collect estimated implementation costs
- DoD Web-based CUI Awareness Training scheduled for release in March 2010



Points of Contact

DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004

Mr. William Cira

Information Security Oversight Office

202-357-5323

William.Cira@nara.gov

Ms. Carroll Lee

Office of the Under Secretary of Defense Intelligence

703-604-1143

Carroll.Lee@osd.mil



Points of Contact

DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004

Ms. Deborah Ross

Office of the Under Secretary of Defense Intelligence
703-604-1143

Carroll.Lee@osd.mil

Mr. Ed Kaufhold

Office of the Under Secretary of Defense Intelligence
703-604-1143

Edward.Kaufhold@osd.mil

Mr. Robert Van Veghel

DTIC

703-767-8240

rvanvegh@dtic.mil



Disclaimer of Endorsement

DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004 DoD Field Activity Since 2004

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.