OPEN HOUSE

Information Security Oversight Office

Protect • Inform • Assess

November 3, 2016 9:30 a.m.–12:30 p.m.

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE

Networking Break

OPEN HOUSE

Information Security Oversight Office

Protect • Inform • Assess

November 3, 2016 9:30 a.m.–12:30 p.m.

ISOO

INFORMATION SECURITY OVERSIGHT OFFICE

Controlled Unclassified Information Program
Mark Riddle, Senior Program Analyst, ISOO

Controlled Unclassified Information

Executive Order 13556

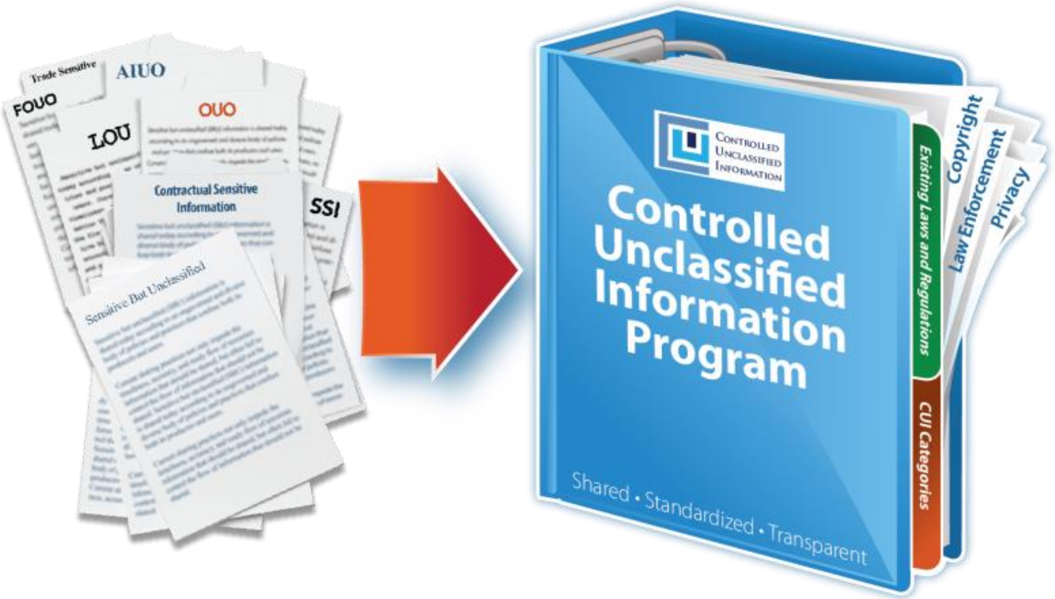
Shared • Standardized • Transparent

Controlled
Unclassified
Information

Information Security Oversight Office (ISOO)

Briefing Outline

- Executive Order 13556
- 32CFR2002 (implementing directive)
- Approach to Contractor Environment
- Phased Implementation
- Understanding the CUI Program

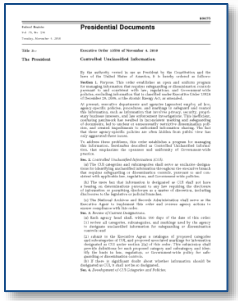

Trade Sensitive
AIUO
FOUO
OUO
LOU
Contractual Sensitive Information
SSI
Sensitive But Unclassified
Controlled Unclassified Information
Controlled Unclassified Information Program
Shared • Standardized • Transparent
Existing Laws and Regulations
CUI Categories
Copyright
Law Enforcement
Privacy

Why is the CUI Program necessary?

Executive departments and agencies apply their own ad-hoc policies and markings to unclassified information that requires safeguarding or dissemination controls, resulting in:

- An inefficient patchwork system with **more than 100 different policies and markings** across the executive branch
- Inconsistent marking and safeguarding of documents
- Unclear or unnecessarily restrictive dissemination policies
- Impediments to authorized information sharing

Executive Order 13556



68675

Federal Register
Vol. 75, No. 216
Tuesday, November 9, 2010

Presidential Documents

Title 3—

The President

Executive Order 13556 of November 4, 2010

Controlled Unclassified Information

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:

Section 1. *Purpose.* This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.

To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice.

Sec. 2. *Controlled Unclassified Information (CUI).*

(a) The CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

(b) The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches.

(c) The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.

Sec. 3. *Review of Current Designations.*

(a) Each agency head shall, within 180 days of the date of this order:

(1) review all categories, subcategories, and markings used by the agency to designate unclassified information for safeguarding or dissemination controls; and

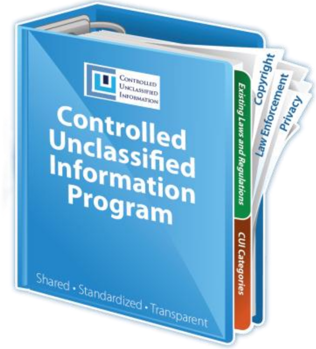
(2) submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI, and proposed associated markings for information designated as CUI under section 2(a) of this order. This submission shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls.

(b) If there is significant doubt about whether information should be designated as CUI, it shall not be so designated.

Sec. 4. *Development of CUI Categories and Policies.*

- Established CUI Program
  - In consultation with affected agencies (CUI Advisory Council)

- Designated an Executive Agent (EA) to implement the E.O. and oversee department and agency actions to ensure compliance.
  - National Archives and Records Administration
  - **Information Security Oversight Office**


Controlled Unclassified Information
Controlled Unclassified Information Program
Shared • Standardized • Transparent
Existing Laws and Regulations
Copyright
Law Enforcement
Privacy
CUI Categories

- An open and uniform program to manage all unclassified information within the executive branch that requires safeguarding and dissemination controls as required by law, regulation, and Government-wide policy

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

CUI Registry

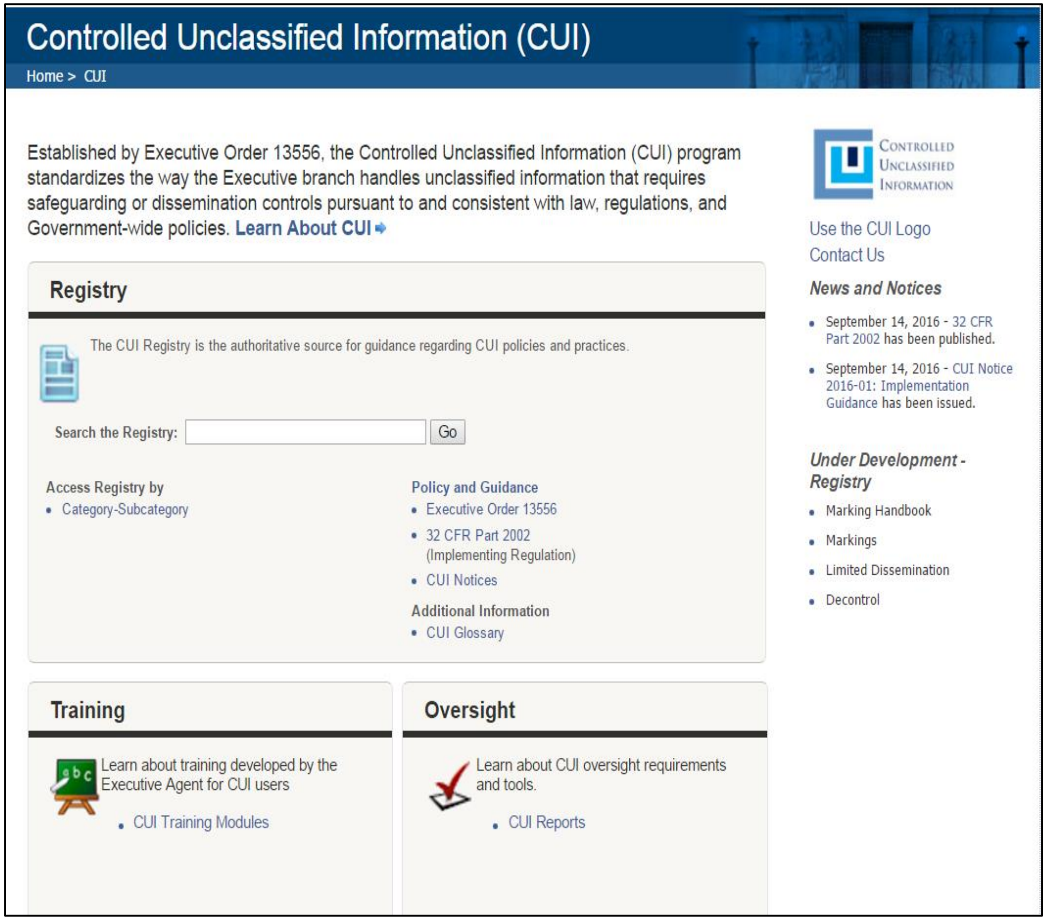
EO 13556 called for a review of the categories, subcategories, and markings currently used by agencies.

Agencies submitted over 2,200 authorities for controlling many types of information.

Information types were grouped together, legal authorities were examined, and a CUI Registry was published.

- 23 Categories
- 84 Sub-categories
- 315 Control citations
- 106 Sanction citations

www.archives.gov/cui



Controlled Unclassified Information (CUI)

Home > CUI

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. Learn About CUI

Registry

The CUI Registry is the authoritative source for guidance regarding CUI policies and practices.

Search the Registry: Go

Access Registry by
- Category-Subcategory

Policy and Guidance
- Executive Order 13556
- 32 CFR Part 2002 (Implementing Regulation)
- CUI Notices

Additional Information
- CUI Glossary

Training

Learn about training developed by the Executive Agent for CUI users
- CUI Training Modules

Oversight

Learn about CUI oversight requirements and tools.
- CUI Reports

Controlled Unclassified Information

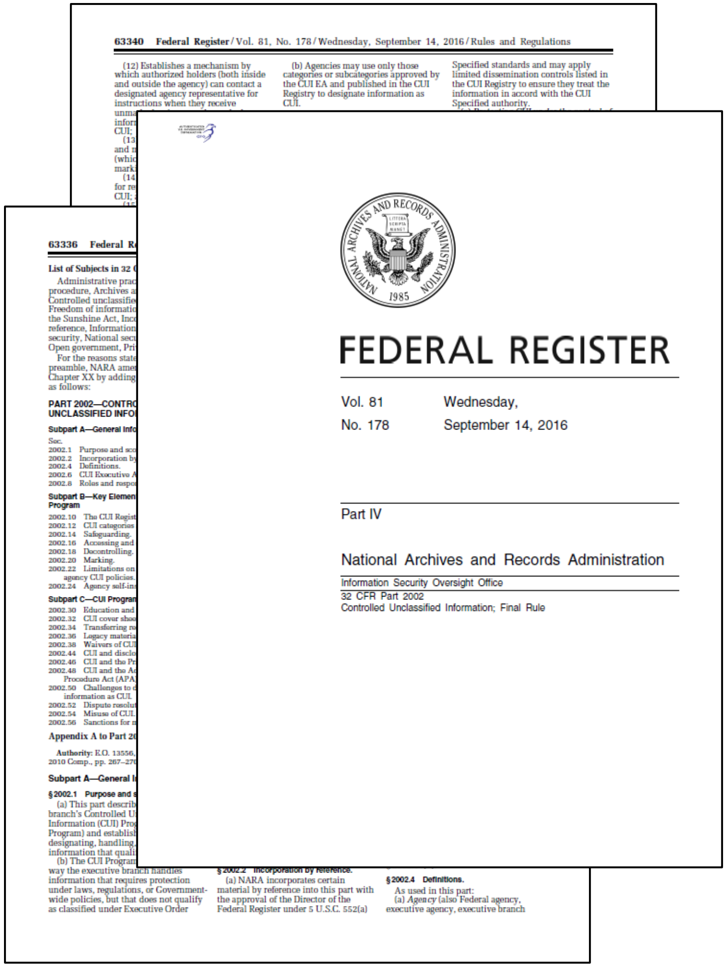
Use the CUI Logo

Contact Us

News and Notices
- September 14, 2016 - 32 CFR Part 2002 has been published.
- September 14, 2016 - CUI Notice 2016-01: Implementation Guidance has been issued.

Under Development - Registry
- Marking Handbook
- Markings
- Limited Dissemination
- Decontrol

32 CFR 2002 (September 14, 2016)



63340 **Federal Register** / Vol. 81, No. 178 / Wednesday, September 14, 2016 / Rules and Regulations

(12) Establishes a mechanism by which authorized holders (both inside and outside the agency) can contact a designated agency representative for instructions when they receive unma
infor
CUI;
(13
and m
(whic
marki
(14
for re
CUI;

(b) Agencies may use only those categories or subcategories approved by the CUI EA and published in the CUI Registry to designate information as CUI.

Specified standards and may apply limited dissemination controls listed in the CUI Registry to ensure they treat the information in accord with the CUI Specified authority.

63336 **Federal R**

List of Subjects in 32 C

Administrative prac
procedure, Archives a
Controlled unclassifie
Freedom of informatio
the Sunshine Act, Inc
reference, Information
security, National secu
Open government, Pri
For the reasons state
preamble, NARA amer
Chapter XX by adding
as follows:

PART 2002—CONTRO UNCLASSIFIED INFO

Subpart A—General Info

Sec.
2002.1 Purpose and sco
2002.2 Incorporation by
2002.4 Definitions.
2002.6 CUI Executive A
2002.8 Roles and respo

Subpart B—Key Elemen Program

2002.10 The CUI Regist
2002.12 CUI categories
2002.14 Safeguarding.
2002.16 Accessing and
2002.18 Decontrolling.
2002.20 Marking.
2002.22 Limitations on agency CUI policies.
2002.24 Agency self-ins

Subpart C—CUI Progran

2002.30 Education and
2002.32 CUI cover shee
2002.34 Transferring re
2002.36 Legacy materia
2002.38 Waivers of CUI
2002.44 CUI and disclo
2002.46 CUI and the Pr
2002.48 CUI and the Ac Procedure Act (APA)
2002.50 Challenges to d information as CUI.
2002.52 Dispute resolut
2002.54 Misuse of CUI.
2002.56 Sanctions for m

Appendix A to Part 20

Authority: E.O. 13556, 2010 Comp., pp. 267–270

Subpart A—General I

§ 2002.1 Purpose and s

(a) This part describ
branch's Controlled U
Information (CUI) Prog
Program) and establish
designating, handling,
information that quali
(b) The CUI Program
way the executive branch handles information that requires protection under laws, regulations, or Government-wide policies, but that does not qualify as classified under Executive Order

§ 2002.2 Incorporation by reference.

(a) NARA incorporates certain material by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 552(a)

§ 2002.4 Definitions.

As used in this part:
(a) *Agency* (also Federal agency, executive agency, executive branch

FEDERAL REGISTER

Vol. 81 Wednesday,
No. 178 September 14, 2016

Part IV

National Archives and Records Administration

Information Security Oversight Office

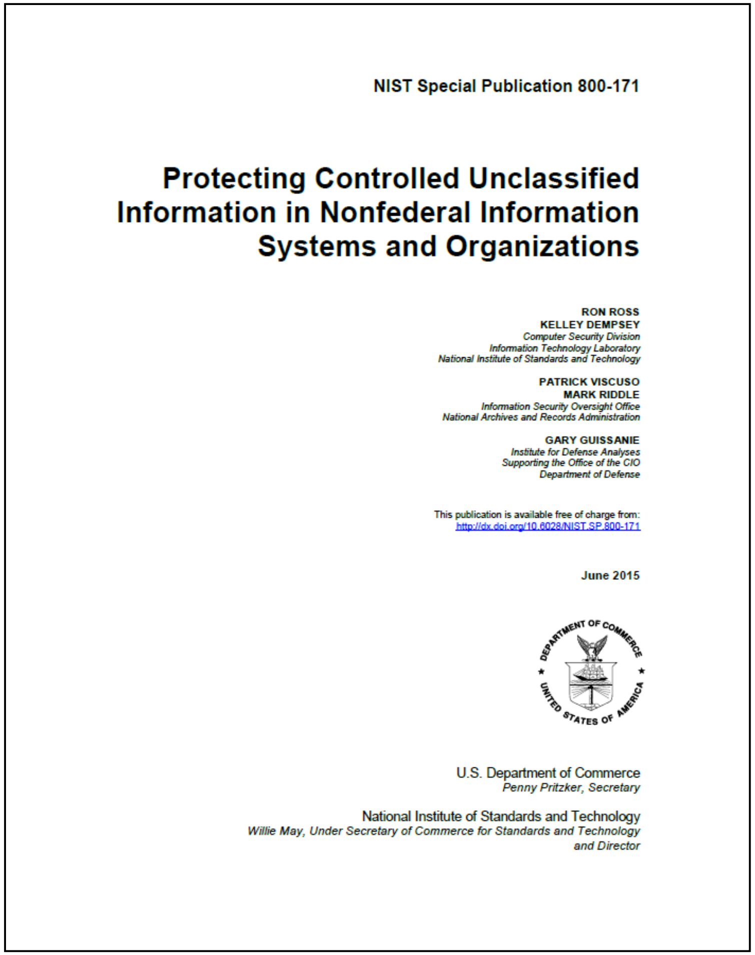
32 CFR Part 2002
Controlled Unclassified Information; Final Rule

- Implements the CUI Program
  - Establishes policy for designating, handling, and decontrolling information that qualifies as CUI
  - Effective : November 14, 2016 (Day 0)
- Describes, defines, and provides guidance on the minimum protections (derived from existing agency practices) for CUI
  - Physical and Electronic Environments
  - Marking
  - Sharing
  - Destruction
  - Decontrol
- Emphasizes unique protections described in law, regulation, and/or Government-wide policies (authorities)

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

NIST Special Publication 800-171

- **Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems.**
- **The NIST 800-171 is intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations.**
- **Establishes requirements for protecting CUI at the Moderate Confidentiality Impact Value.**
- **Non-tailorable requirements**
- **Flexibility in how to meet requirements**



NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
KELLEY DEMPSEY
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

PATRICK VISCUSO
MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

GARY GUISSANIE
Institute for Defense Analyses
Supporting the Office of the CIO
Department of Defense

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-171

June 2015

DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

U.S. Department of Commerce
Penny Pritzker, Secretary

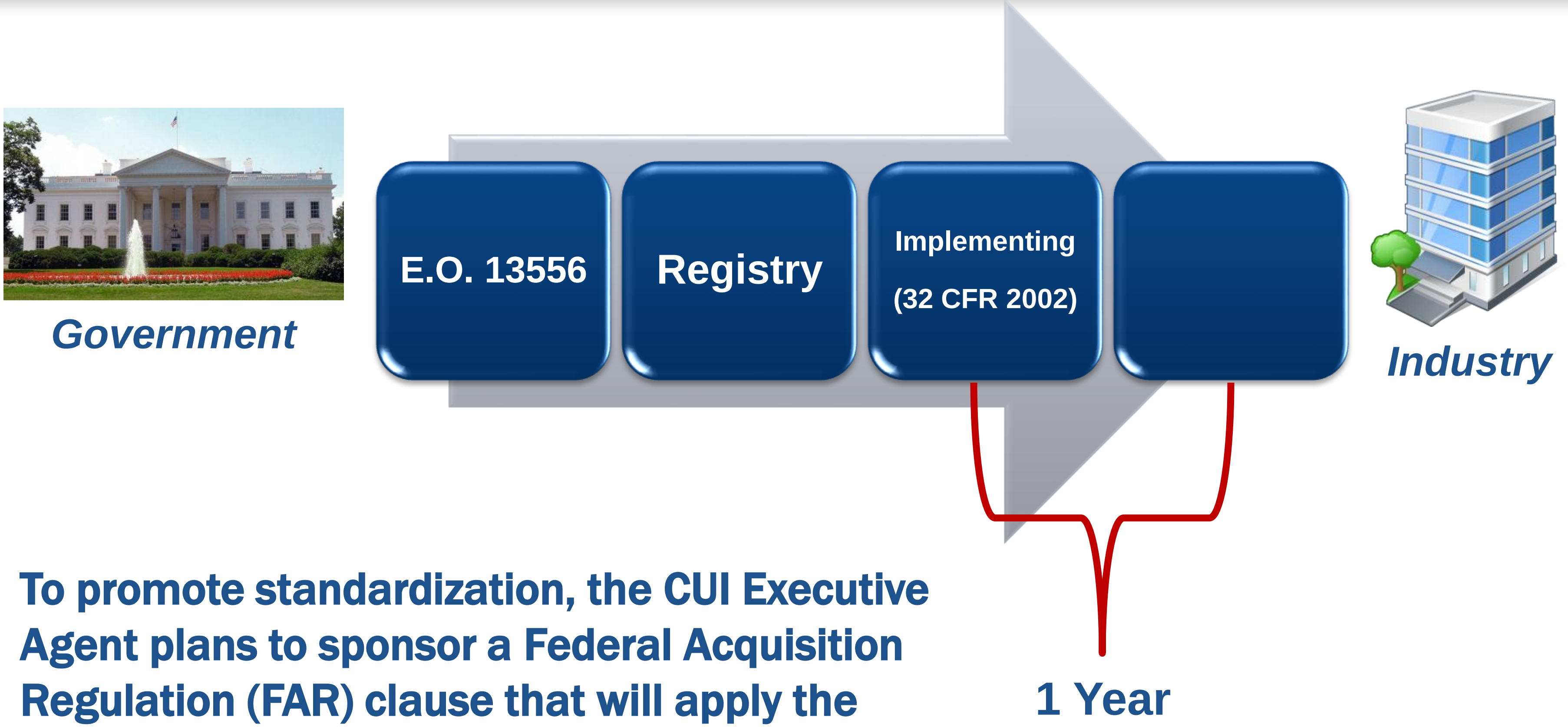
National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

When to use the NIST SP 800-171

- Use the NIST SP 800-171 when a non-Federal entity:
  - Receives CUI incidental to providing a service or product to the Government outside or processing services. Examples: producing a study, conducting research, creating a training program, building an aircraft or ship, etc.
  - In these instances, the Government is only concerned with the confidentiality of the information and the CUI is regarded as the asset requiring protection.

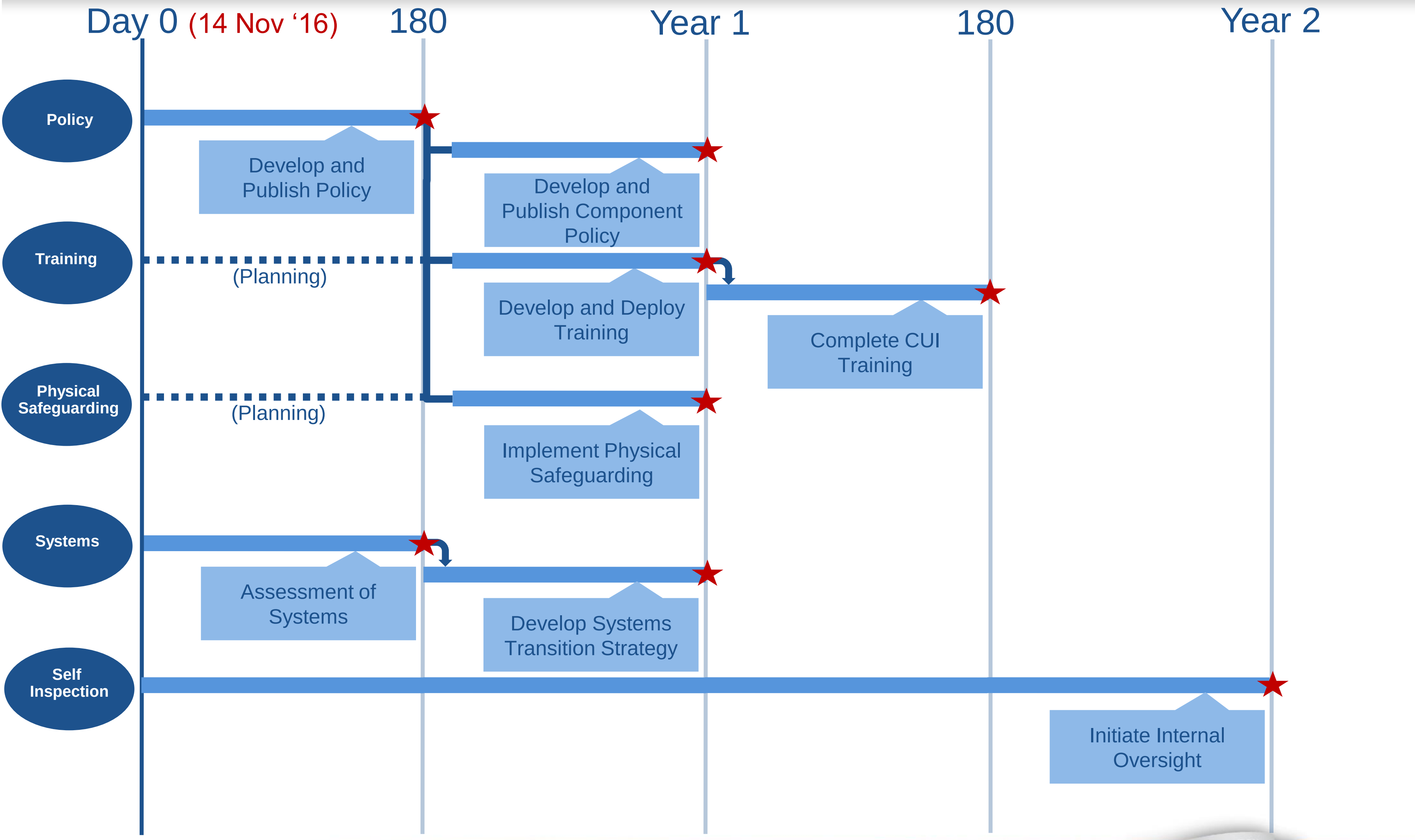
- Do NOT use the NIST SP 800-171 when a non-Federal entity:
  - Collects or maintains CUI as part of a Government function (e.g., census takers or records storage).
  - Builds an information system or operates an information system for the Government (an email provider, or payroll system).
  - Provides processing services for the Government (a cloud service provider)
  - In these instances, the Government has a concern in the confidentiality, integrity, and availability of the information system and the system is the asset requiring protection.
  - Agencies may require these systems to meet additional requirements the agency sets for its own internal systems.

Federal Acquisition Regulation



To promote standardization, the CUI Executive Agent plans to sponsor a Federal Acquisition Regulation (FAR) clause that will apply the requirements contained in the 32 CFR Part 2002 and NIST SP 800-171 to industry.

Implementation of the CUI Program



Day 0 (14 Nov '16)
180
Year 1
180
Year 2
Policy
Develop and Publish Policy
Develop and Publish Component Policy
Training
(Planning)
Develop and Deploy Training
Complete CUI Training
Physical Safeguarding
(Planning)
Implement Physical Safeguarding
Systems
Assessment of Systems
Develop Systems Transition Strategy
Self Inspection
Initiate Internal Oversight

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

Additional Implementation Concerns

- Program Management
  - Senior Agency Official, Program Manager, internal planning teams
- Incident Management
  - Reporting, Mitigation, and Preventing Recurrence
- Contracts & Agreements (agencies and non-federals)
  - Guidance given to external entities on how to handle CUI
  - Limitations on Applicability of Agency Policies

Understanding the CUI Program

- CUI Basic versus CUI Specified
- Limitations of Agency Policy
- Controlled Environments
- Systems Requirements: Moderate
- Marking CUI
  - Banner, Designator, Specified, Portion, Limited Dissemination Control Markings
  - Bulk & Systems (splash screens)
  - Legacy Information, derivative use.
  - Handbook & Coversheets
- Destruction

Two types of CUI: Basic and Specified

- CUI Basic = LRGWP identifies an information type and says protect it.

Examples include: Agriculture, Ammonium Nitrate, Water Assessments, Emergency Management, Bank Secrecy, Budget, Comptroller General, Geodetic Product Information, Asylee, Visas, Information Systems Vulnerabilities, Terrorist Screening, Informant, Privilege, Victim, Death Records

- CUI Specified = LRGWP identifies an information type and says to protect it, and also includes one or more specific handling standards for that information.

Examples include: Sensitive Security Information, Student Records, Personnel, Source Selection, Nuclear, Safeguards Information, NATO Restricted, NATO Unclassified, Federal Grand Jury, Witness Protection, DNA, Criminal History Records, Financial Records, Export Control, Protected Critical Infrastructure Information, Controlled Technical Information

Limitations on applicability

Limitations on applicability of agency CUI policies

- Agency policies pertaining to CUI do not apply to entities outside that agency unless the CUI Executive Agent approves their application and publishes them in the CUI Registry.
- Agencies may not levy any requirements in addition to those contained in the Order, this Part, or the CUI Registry when entering into contracts, treaties, or other agreements about handling CUI by entities outside of that agency.

General Safeguarding Policy

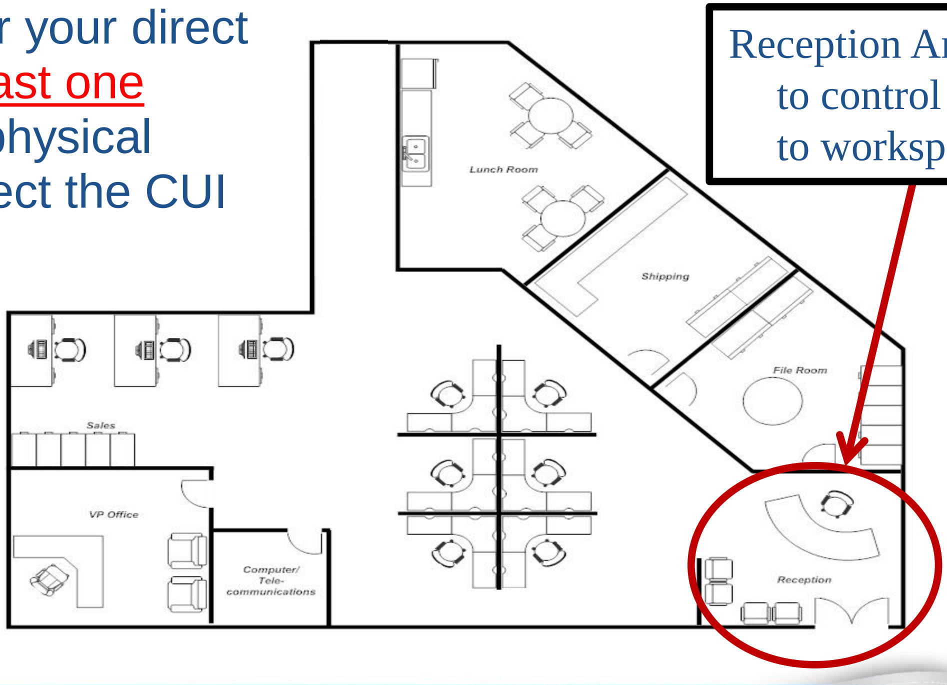
- Agencies must safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders.
  - For categories designated as CUI Specified, personnel must also follow the procedures in the underlying law, regulation, or Government-wide policy that established the specific category or subcategory involved.

- Safeguarding measures that are authorized or accredited for classified information are sufficient for safeguarding CUI.

Controlled Environments

Controlled environment is any area or space an authorized holder deems to have adequate physical or procedural controls (*e.g.*, barriers and managed access controls) for protecting CUI from unauthorized access or disclosure.

- When outside a controlled environment, you must keep the CUI under your direct control or protect it with at least one physical barrier. You or the physical barrier must reasonably protect the CUI from unauthorized access or observation.



Reception Area used to control access to workspace.

System Requirements: Moderate

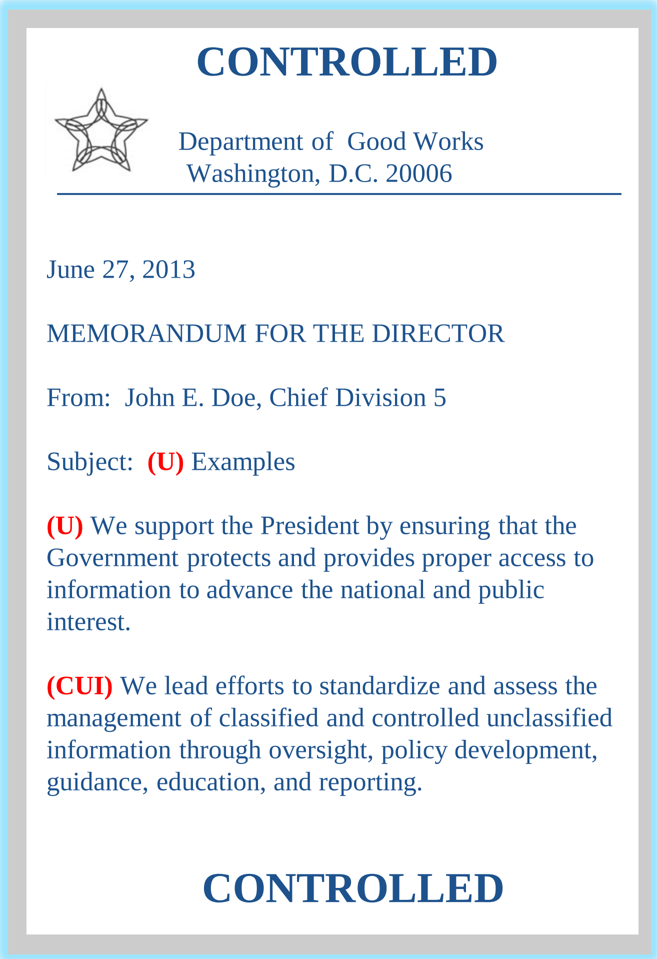
- Systems that store or process CUI must be protected at the Moderate Confidentiality Impact Value.
  - FIPS PUB 199 & 200
  - NIST SP-800-53 (Risk Based Tailoring)

- Moderate = The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. (FIPS PUB 199).
  - A serious adverse effect means that, for example, the loss of confidentiality might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries

Marking CUI

- Agencies must uniformly and conspicuously apply CUI markings to all CUI prior to disseminating it unless otherwise specifically permitted by the CUI Executive Agent.

- The CUI banner marking must appear, at a minimum, at the top center of each page containing CUI



CONTROLLED

Department of Good Works
Washington, D.C. 20006

June 27, 2013

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

Subject: **(U)** Examples

(U) We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

(CUI) We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

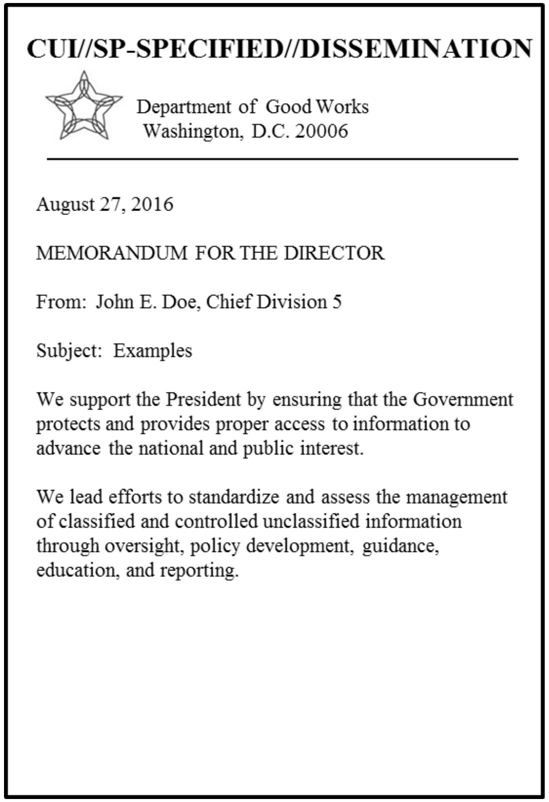
CONTROLLED

Portion Marking = Best Practice

Marking CUI: Banner Marking

The CUI Banner Marking may include up to three elements:

- The CUI Control Marking (mandatory) may consist of consist of either the word “CONTROLLED” or the acronym “CUI.”
- CUI Category or Subcategory Markings (mandatory for (mandatory for CUI Specified). CUI Control Markings Markings and Category Markings are separated by two by two forward slashes (//). When including multiple multiple categories or subcategories in a Banner Marking they are separated by a single forward slash slash (/).
- Limited Dissemination Control Markings. CUI Control Control Markings and Category Markings are separated separated from Limited Dissemination Controls Markings by a double forward slash (//).



CUI//SP-SPECIFIED//DISSEMINATION

Department of Good Works
Washington, D.C. 20006

August 27, 2016

MEMORANDUM FOR THE DIRECTOR

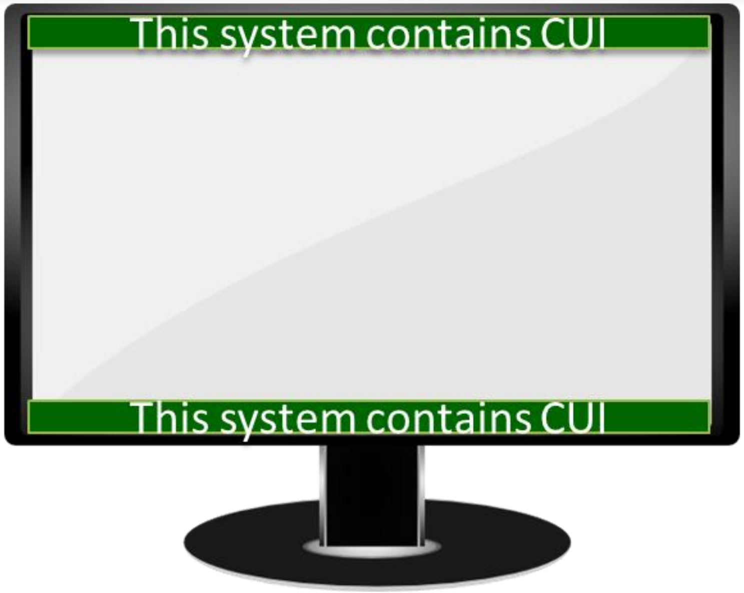
From: John E. Doe, Chief Division 5

Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

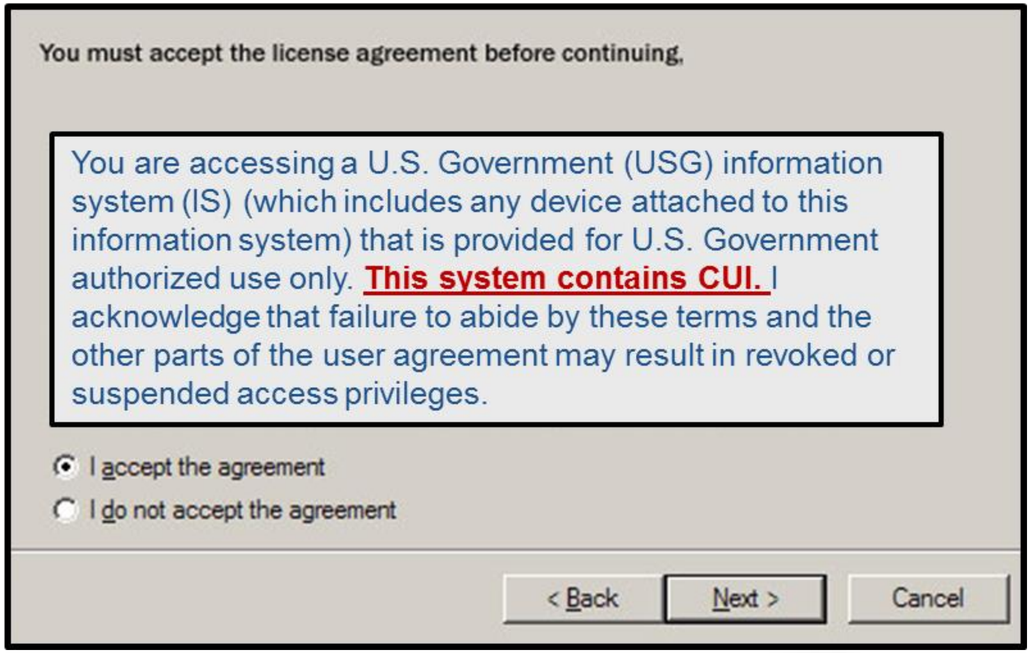
We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

Bulk & System Markings



Agencies may authorize or require the use of alternate CUI indicators on IT systems, websites, browsers, or databases through agency CUI policy. These may be used to alert users of the presence of CUI where use of markings has been waived by the agency head.

This box contains CUI
This box contains CUI



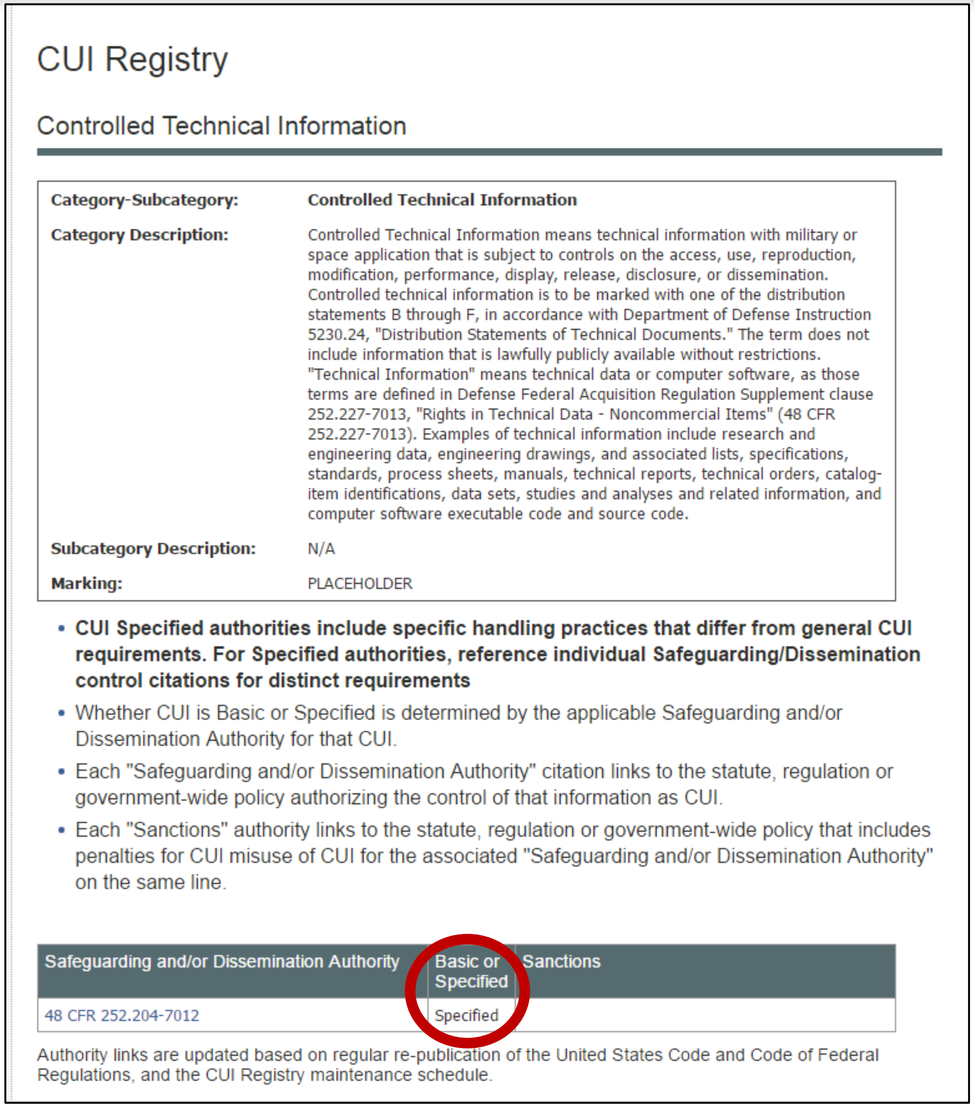
You must accept the license agreement before continuing.

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only. **This system contains CUI.** I acknowledge that failure to abide by these terms and the other parts of the user agreement may result in revoked or suspended access privileges.

● I accept the agreement

○ I do not accept the agreement

CUI Specified



CUI Registry

Controlled Technical Information

Category-Subcategory:	**Controlled Technical Information**
Category Description:	Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
Subcategory Description:	N/A
Marking:	PLACEHOLDER

- **CUI Specified authorities include specific handling practices that differ from general CUI requirements. For Specified authorities, reference individual Safeguarding/Dissemination control citations for distinct requirements**
- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizing the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CUI for the associated "Safeguarding and/or Dissemination Authority" on the same line.

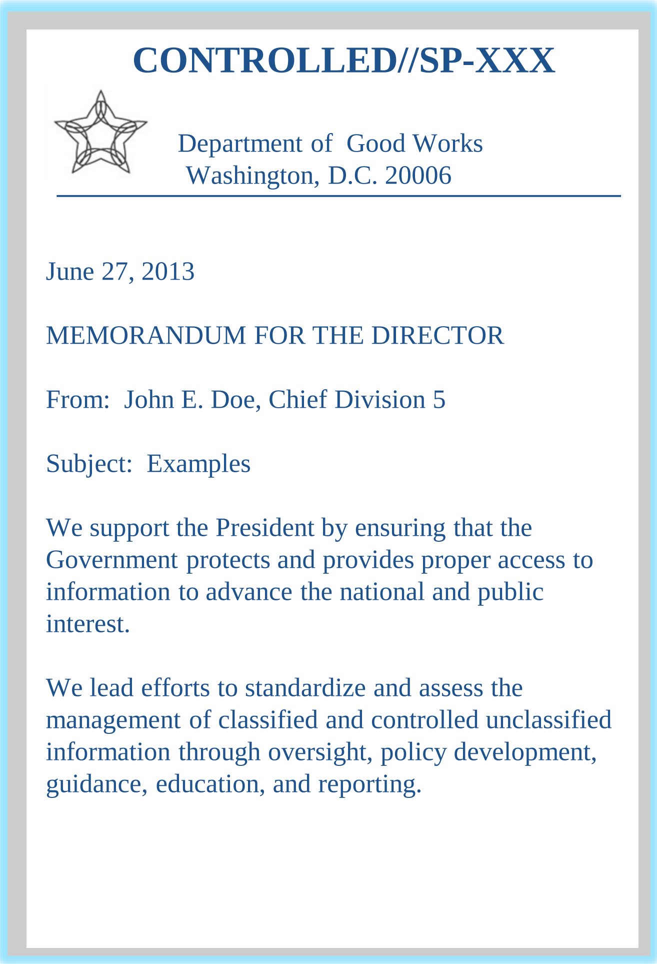
Safeguarding and/or Dissemination Authority	Basic or Specified	Sanctions
48 CFR 252.204-7012	Specified	

Authority links are updated based on regular re-publication of the United States Code and Code of Federal Regulations, and the CUI Registry maintenance schedule.

In the CUI Registry, if the authority that relates to the information is indicated to be specified, documents **must** be marked to indicate that CUI Specified is present in the document.

Add "SP-" before any category/subcategory markings where the authority is followed by an asterisk.

Marking CUI Specified



CONTROLLED//SP-XXX

Department of Good Works
Washington, D.C. 20006

June 27, 2013

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

Subject: Examples

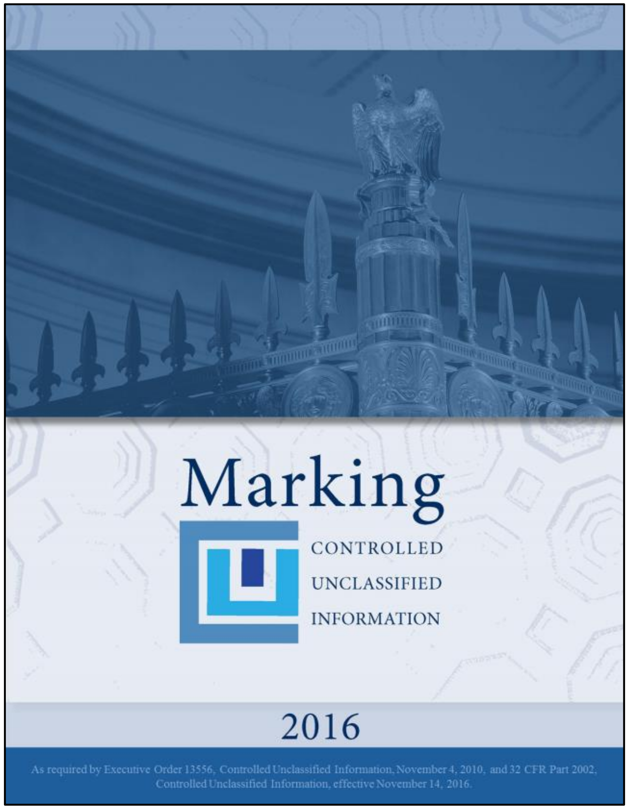
We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

"SP-" Indicates that an authority contains specific safeguarding or dissemination measures.

Recipients are encouraged to reference the underlying, "specified," authority(s) for specific handling guidance.

Marking Handbook & Cover Sheets

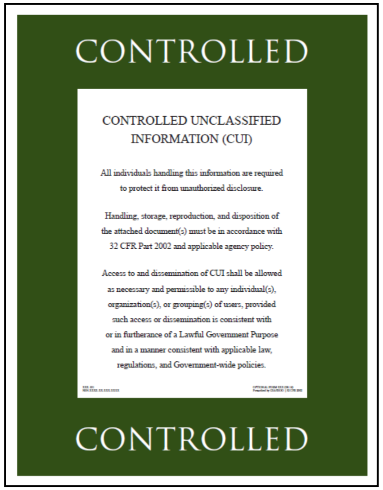


Marking

CONTROLLED UNCLASSIFIED INFORMATION

2016

As required by Executive Order 13556, Controlled Unclassified Information, November 4, 2010, and 32 CFR Part 2002, Controlled Unclassified Information, effective November 14, 2016.



CONTROLLED

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

All individuals handling this information are required to protect it from unauthorized disclosure.

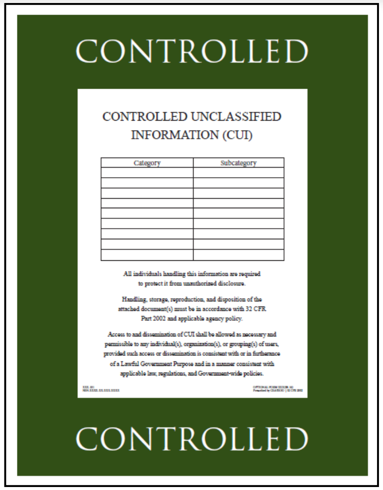
Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of CUI shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

XXX. 101
NSN XXXX-XX-XXX-XXXX

OPTIONAL FORM XXX (08-16)
Prescribed by GSA/ISOO | 32 CFR 2002

CONTROLLED



CONTROLLED

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Category	Subcategory

All individuals handling this information are required to protect it from unauthorized disclosure.

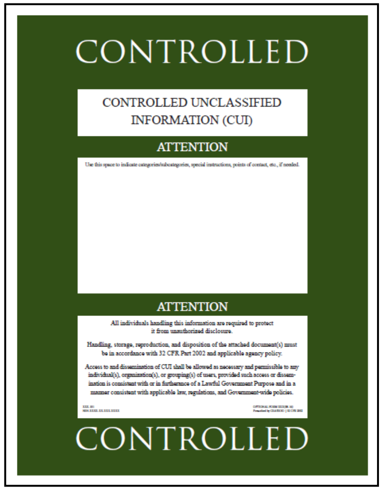
Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of CUI shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

XXX. 101
NSN XXXX-XX-XXX-XXXX

OPTIONAL FORM XXX (08-16)
Prescribed by GSA/ISOO | 32 CFR 2002

CONTROLLED



CONTROLLED

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

ATTENTION

Use this space to indicate categories/subcategories, special instructions, points of contact, etc., if needed.

ATTENTION

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of CUI shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

XXX. 101
NSN XXXX-XX-XXX-XXXX

OPTIONAL FORM XXX (08-16)
Prescribed by GSA/ISOO | 32 CFR 2002

CONTROLLED

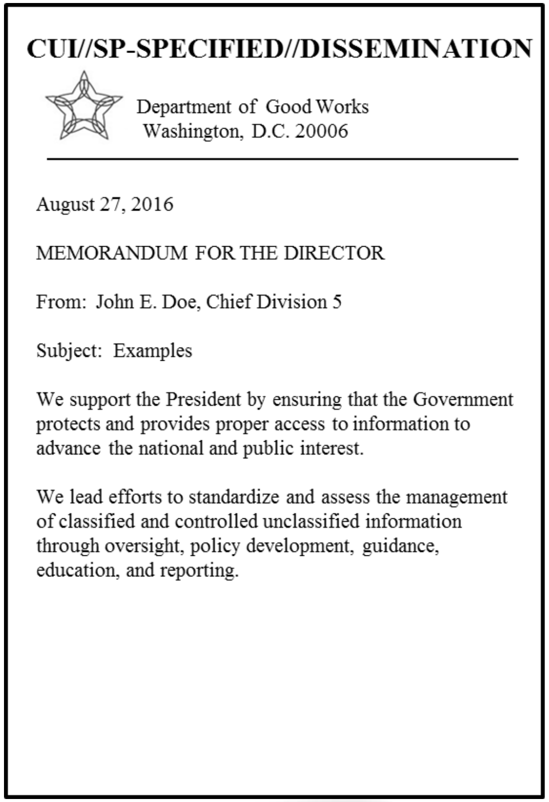
Legacy Information and Markings

Trade Sensitive
AIUO
FOUO
LOU
OUO
Contractual Sensitive Information
SSI
Sensitive But Unclassified

Legacy Information is unclassified information that an agency marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program.

All legacy information is not automatically CUI. Agencies must examine and determine what legacy information qualifies as CUI

Discontinue all use of legacy markings



CUI//SP-SPECIFIED//DISSEMINATION

Department of Good Works
Washington, D.C. 20006

August 27, 2016

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

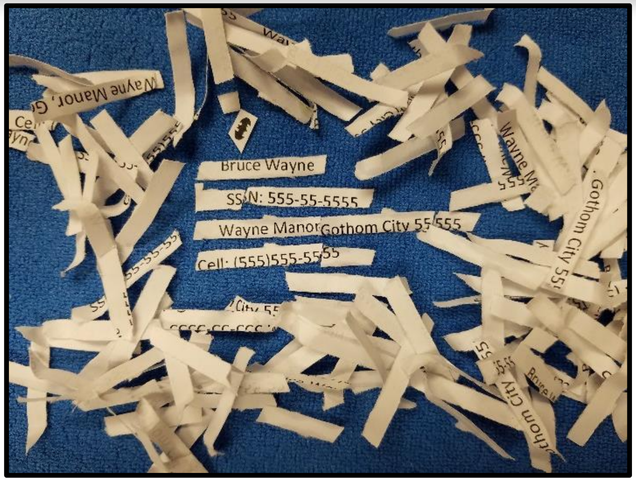
Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

Destruction

- When destroying CUI, including in electronic form, you must do so in a manner that makes it unreadable, indecipherable, and irrecoverable, using any of the following:
  - Guidance for destruction in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800-88, Guidelines for Media Sanitization;
  - Any method of destruction approved for Classified National Security Information
  - Any specific destruction methods required by law, regulation, or Government-wide policy for that item.

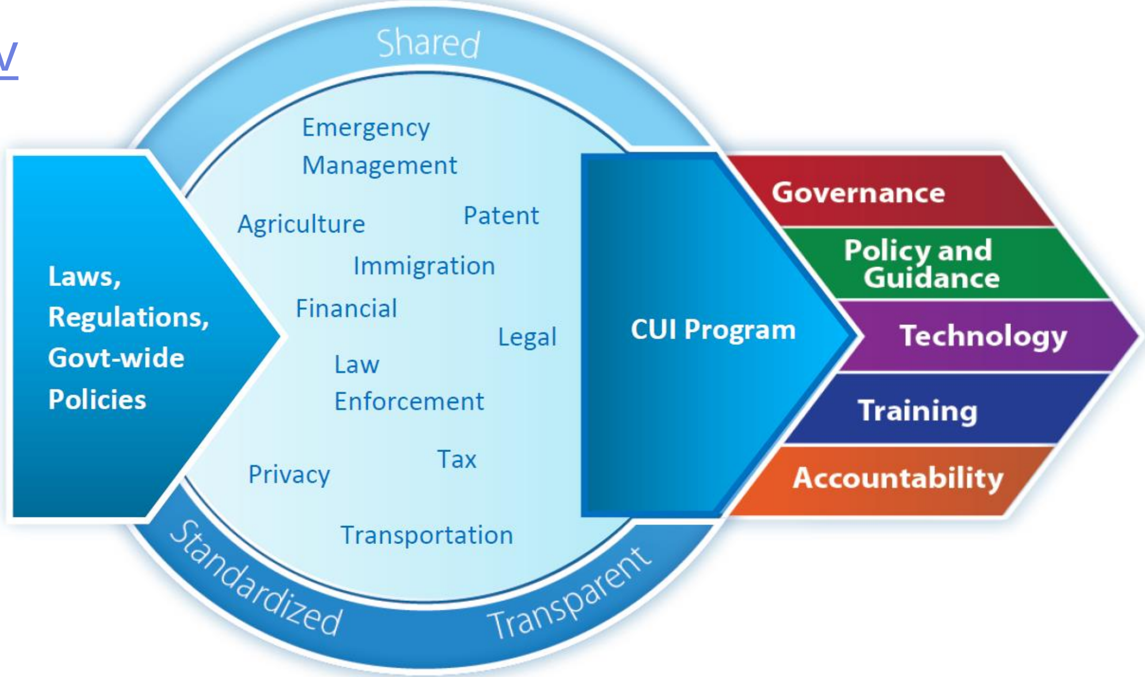


Destroy paper using cross cut shredders that produce particles that are 1mm by 5 mm.

Questions?

Mark Riddle
Lead for Implementation and Oversight
mark.riddle@nara.gov

Bryan M. Oklin
Attorney Advisor
bryan.oklin@nara.gov



Controlled Unclassified Information

Executive Order 13556

Shared • Standardized • Transparent

Controlled
Unclassified
Information

Information Security Oversight Office (ISOO)

OPEN HOUSE

Information Security Oversight Office

Protect • Inform • Assess

November 3, 2016 9:30 a.m.–12:30 p.m.

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE

Interagency Security Classification Appeals Panel (ISCAP) Overview
William Cira, Acting Director, ISOO

What is the ISCAP?

- Interagency Security Classification Appeals Panel
- Created by President Clinton in Executive Order 12958 in 1995
- The ISCAP provides the public and users of the classification system with a forum for further review of classification decisions
- Four functions:
  - Decide on appeals for classification challenges
  - Approve exemptions to declassification at 25, 50, and 75 years
  - Decide on mandatory declassification review (MDR) appeals
  - Inform senior agency officials and the public of its decisions

Membership of the ISCAP

- National Security Council:
  - John Fitzpatrick (Chair), Senior Director, Records Access and Information Security Management
- Department of Defense:
  - Garry P. Reid, Director for Defense Intelligence, Office of the Deputy Under Secretary of Defense (Intelligence and Security)
- Department of Justice:
  - Mark Bradley, Director of FOIA, Declassification, and Pre-Publication Review, National Security Division
- Department of State:
  - Nicholas Murphy, Office of Information Programs and Services
- National Archives and Records Administration
  - Sheryl Shenberger, Director, National Declassification Center
- Office of the Director of National Intelligence
  - Robert Warrington, Information and Data Management Group
- Central Intelligence Agency (for discussions regarding CIA information only)
  - Joseph Lambert, Director, Information Management Services

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

Membership and Staffing

- ISCAP members are senior agency leaders appointed by agency heads
- ISCAP members appoint Liaisons to meet on a biweekly basis
  - Liaisons are experienced senior managers of the records and information staffs of agencies
- The Director of ISOO is the Executive Secretary of the ISCAP
- The ISCAP Staff consists of staff members of ISOO
  - One Senior Program Analyst, five Program Analysts
- ISCAP records are Presidential records, covered by specific release protections established by the Presidential Records Act

Classification Challenges

- Section 1.8 of the Order encourages any authorized holder of classified information to challenge the classification of improperly classified information
- The Order requires agencies to have a formal system for the adjudication and appeal of classification challenges
- The ISCAP is the highest level of appeal for classification challenges
- In 2014, the ISCAP received and decided upon one classification challenge: the Sarwar Jan intelligence report

Declassification Guides

- Agencies describe their declassification exemptions in declassification guides, which are reviewed, amended, and approved by the ISCAP
- Guides must be updated at least every five years: 2017 is the next review cycle
- 23 agencies have received approval from the ISCAP to exempt information from automatic declassification at 25 years:
  - 20 agencies may exempt specific information from declassification at 50 years (information from 1972 and before)
  - 3 agencies have the ability to exempt *very specific* information from declassification at 75 years (from 1947 and before)
  - See ISOO Notice 2015-05, “Agencies Eligible to Receive Referrals from Automatic Declassification at 25, 50, and 75 Years.”

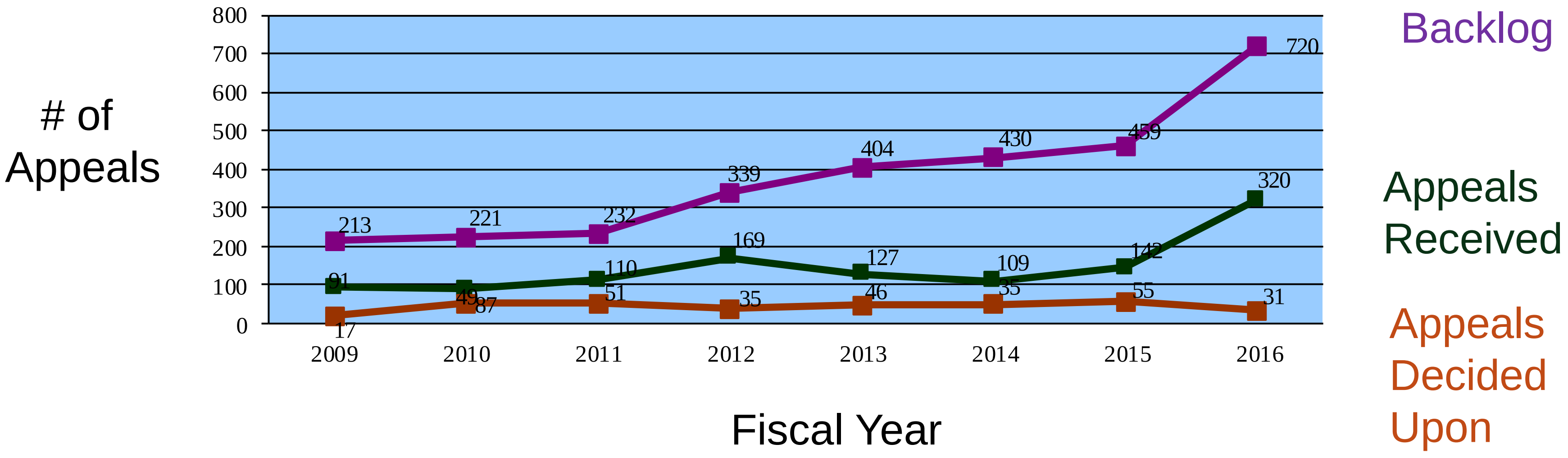
MDR Appeals to the ISCAP

- Mandatory Declassification Review (MDR) requests may be appealed to the ISCAP after the agency has made an appeal decision *or if the requester did not receive a response after one year or a response to an appeal after 180 days*
  - Agencies must continue to process MDR requests that have been appealed to the ISCAP due to the expiration of a response deadline
- Received in FY 2016: 320 appeals (a new record)
- Decided in FY 2016: 31 MDR appeals
  - 190 documents
  - 5150 pages (a new record)
  - 272 minutes of motion picture film (a new record)

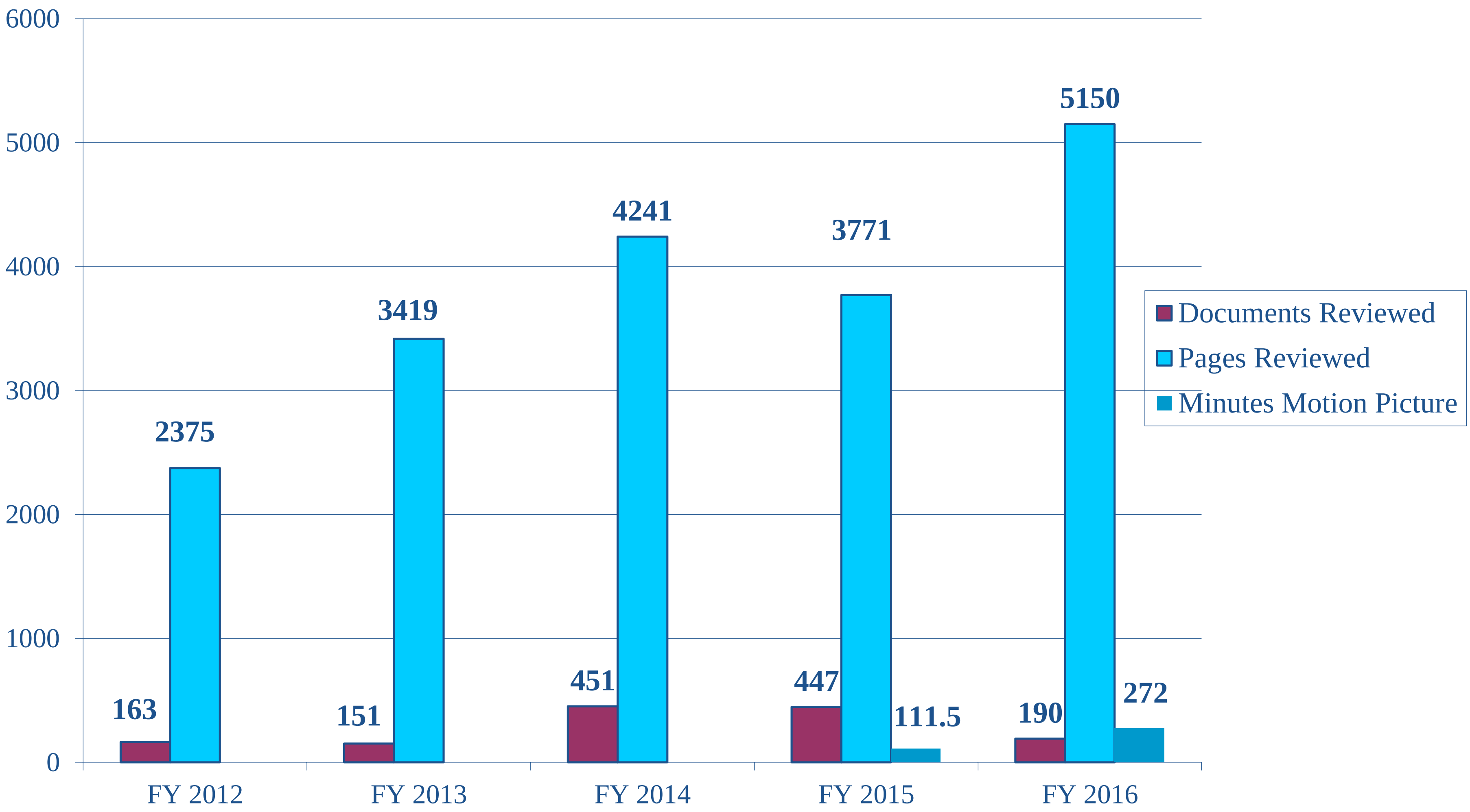
Agency Interaction with the ISCAP

- ISCAP Staff will request responsive materials from agencies when appeals are received
- ISOO Notice 2013-03, “Processing of MDR Requests Appealed to the ISCAP:” continue processing requests that have been appealed to the ISCAP and notify the ISCAP Staff if additional information is later released
- Coordination during ISCAP deliberations
- Decision letters to agency Senior Agency Officials
- Section 3.1(i): “When making decisions under sections 3.3, 3.4, and 3.5 of this order, agencies shall consider the final decisions of the Panel.”

ISCAP Appeals, FY 2009-2016



Comparison of ISCAP Activity



INFORMATION SECURITY OVERSIGHT OFFICE

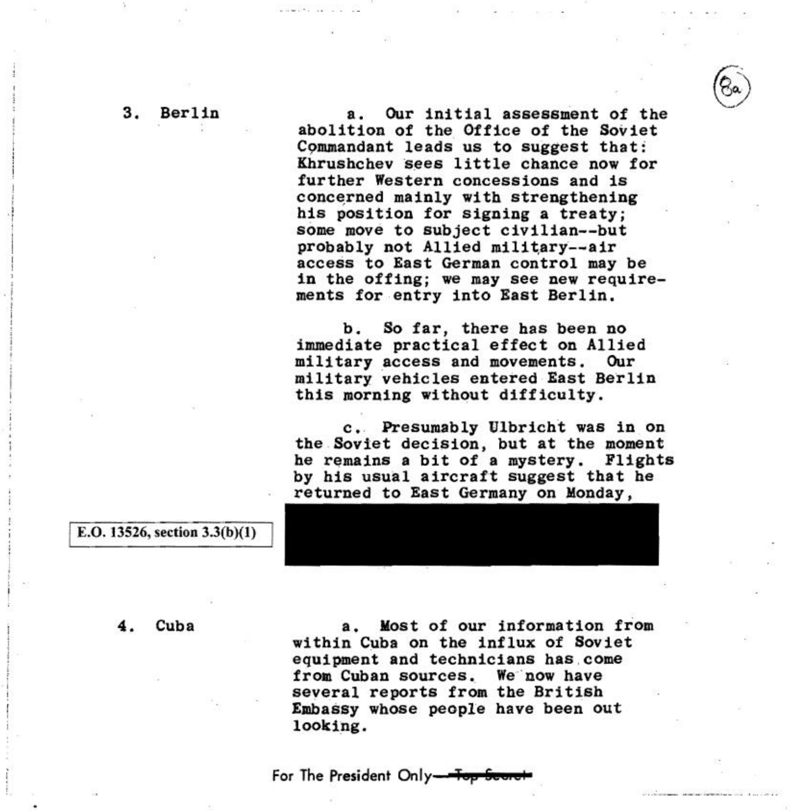
Appeal Selection Criteria

- ISCAP not bound by “first in, first out”
- Factors for appeal selection described on ISCAP website:
  - **Age:** ISCAP is committed to resolving old appeals
  - **Type of appellant:** National Security Archive, or new appellant seeking a single document?
  - **Declassification breakthroughs:** NATO expansion in the 1990s (new topic) vs. Soviet space program (frequent topic)
  - **Size and complexity:** smaller, straightforward appeals may be discussed among large, complex appeals
  - **Self-prioritization** by appellant
  - **Type of appeal:** priority to rare classification challenges

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

How the ISCAP Works

- The ISCAP Liaisons have two three-hour meetings each month
- The ISCAP Staff prepare classified briefing books containing redaction proposals for review and discussion
- ISCAP Members vote on proposals discussed in Liaisons meetings



8a

3. Berlin

a. Our initial assessment of the abolition of the Office of the Soviet Commandant leads us to suggest that: Khrushchev sees little chance now for further Western concessions and is concerned mainly with strengthening his position for signing a treaty; some move to subject civilian--but probably not Allied military--air access to East German control may be in the offing; we may see new requirements for entry into East Berlin.

b. So far, there has been no immediate practical effect on Allied military access and movements. Our military vehicles entered East Berlin this morning without difficulty.

c. Presumably Ulbricht was in on the Soviet decision, but at the moment he remains a bit of a mystery. Flights by his usual aircraft suggest that he returned to East Germany on Monday,

E.O. 13526, section 3.3(b)(1)

[redacted]

4. Cuba

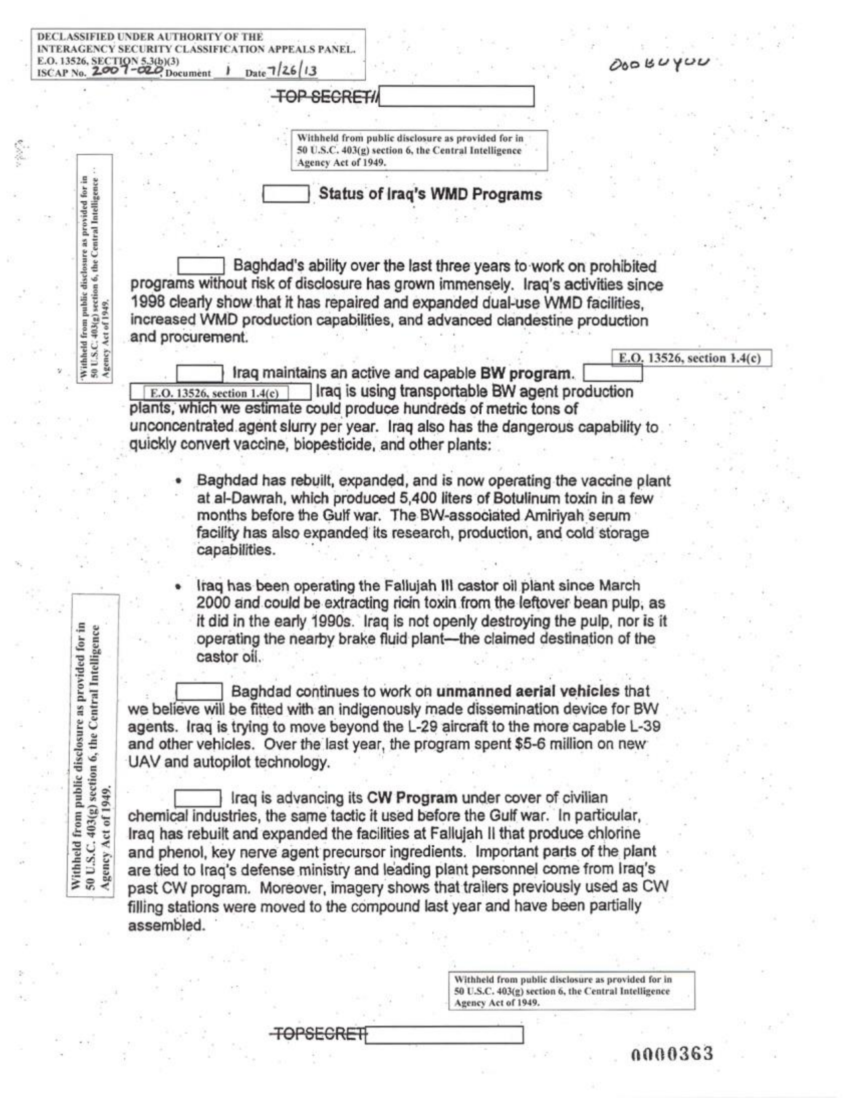
a. Most of our information from within Cuba on the influx of Soviet equipment and technicians has come from Cuban sources. We now have several reports from the British Embassy whose people have been out looking.

For The President Only—~~Top Secret~~

From a President's Intelligence Checklist, 1962

The ISCAP Release Process

- The ISCAP Staff prepare declassified documents for public release
- Some information may be redacted under an agency’s statutory authority
- All redaction reasons are indicated on the released documents
- Documents are released to the appellant and originating agency and posted on the ISCAP website



DECLASSIFIED UNDER AUTHORITY OF THE
INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL.
E.O. 13526, SECTION 5.3(b)(3)
ISCAP No. 2007-020, Document 1 Date 7/26/13

000BUYOU

~~TOP SECRET//~~ [redacted]

Withheld from public disclosure as provided for in 50 U.S.C. 403(g) section 6, the Central Intelligence Agency Act of 1949.

Withheld from public disclosure as provided for in 50 U.S.C. 403(g) section 6, the Central Intelligence Agency Act of 1949.

[redacted] **Status of Iraq's WMD Programs**

[redacted] Baghdad's ability over the last three years to work on prohibited programs without risk of disclosure has grown immensely. Iraq's activities since 1998 clearly show that it has repaired and expanded dual-use WMD facilities, increased WMD production capabilities, and advanced clandestine production and procurement.

E.O. 13526, section 1.4(c)

[redacted] Iraq maintains an active and capable **BW program.** [redacted] E.O. 13526, section 1.4(c) [redacted] Iraq is using transportable BW agent production plants, which we estimate could produce hundreds of metric tons of unconcentrated agent slurry per year. Iraq also has the dangerous capability to quickly convert vaccine, biopesticide, and other plants:

- Baghdad has rebuilt, expanded, and is now operating the vaccine plant at al-Dawrah, which produced 5,400 liters of Botulinum toxin in a few months before the Gulf war. The BW-associated Amiriyah serum facility has also expanded its research, production, and cold storage capabilities.
- Iraq has been operating the Fallujah III castor oil plant since March 2000 and could be extracting ricin toxin from the leftover bean pulp, as it did in the early 1990s. Iraq is not openly destroying the pulp, nor is it operating the nearby brake fluid plant—the claimed destination of the castor oil.

Withheld from public disclosure as provided for in 50 U.S.C. 403(g) section 6, the Central Intelligence Agency Act of 1949.

[redacted] Baghdad continues to work on **unmanned aerial vehicles** that we believe will be fitted with an indigenously made dissemination device for BW agents. Iraq is trying to move beyond the L-29 aircraft to the more capable L-39 and other vehicles. Over the last year, the program spent $5-6 million on new UAV and autopilot technology.

[redacted] Iraq is advancing its **CW Program** under cover of civilian chemical industries, the same tactic it used before the Gulf war. In particular, Iraq has rebuilt and expanded the facilities at Fallujah II that produce chlorine and phenol, key nerve agent precursor ingredients. Important parts of the plant are tied to Iraq's defense ministry and leading plant personnel come from Iraq's past CW program. Moreover, imagery shows that trailers previously used as CW filling stations were moved to the compound last year and have been partially assembled.

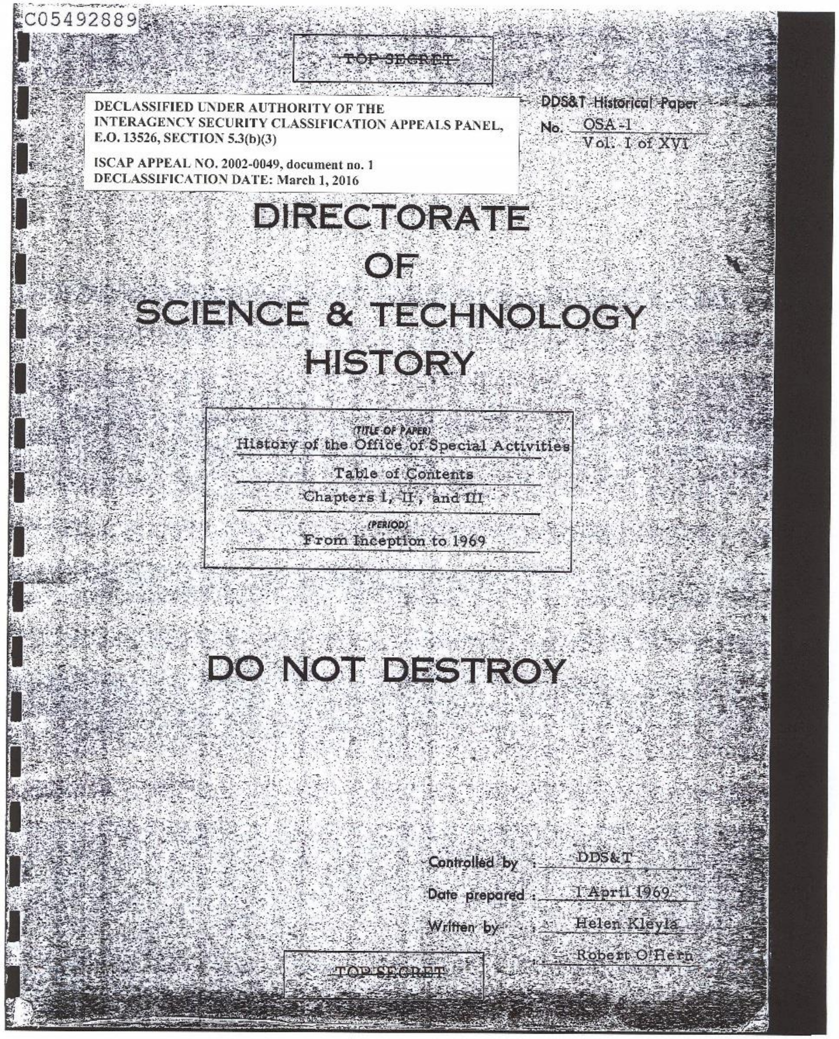
Withheld from public disclosure as provided for in 50 U.S.C. 403(g) section 6, the Central Intelligence Agency Act of 1949.

~~TOPSECRET~~ [redacted]

0000363

2002-0049: U-2 and A-12 Oxcart

- 16-volume History of the Office of Special Activities at CIA
- U-2 and A-12 Oxcart reconnaissance aircraft, to 1969
- Required close coordination with Air Force, NRO, and CIA
- Decided upon in FY 2016: 2577 pages



C05492889

~~TOP SECRET~~

DECLASSIFIED UNDER AUTHORITY OF THE
INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL,
E.O. 13526, SECTION 5.3(b)(3)

ISCAP APPEAL NO. 2002-0049, document no. 1
DECLASSIFICATION DATE: March 1, 2016

DDS&T Historical Paper
No. OSA -1
Vol. I of XVI

DIRECTORATE
OF
SCIENCE & TECHNOLOGY
HISTORY

(TITLE OF PAPER)
History of the Office of Special Activities
Table of Contents
Chapters I, II, and III
(PERIOD)
From Inception to 1969

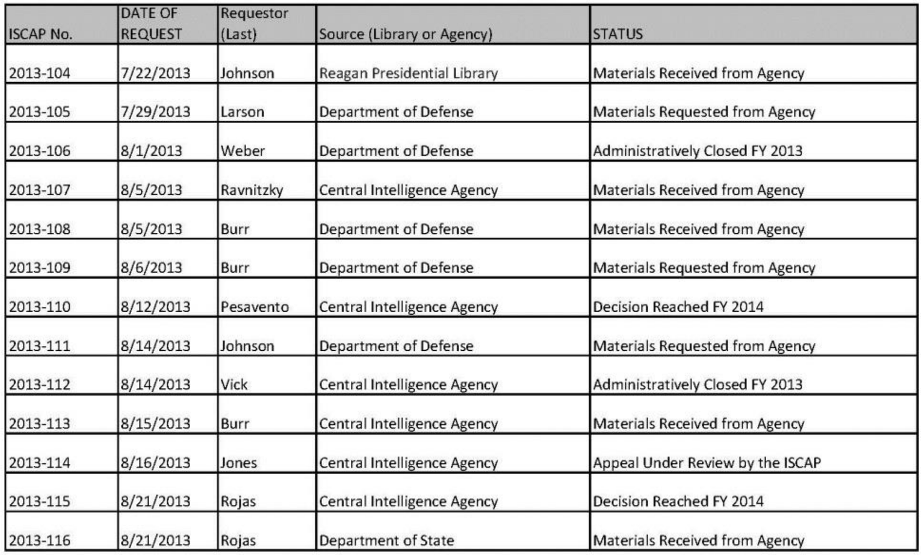
DO NOT DESTROY

Controlled by : DDS&T
Date prepared : 1 April 1969
Written by : Helen Kleyla
: Robert O'Hern

~~TOP SECRET~~

ISCAP Appeals Status Log

- Available on ISCAP website as an Excel spreadsheet
- Lists all appeals active in the Obama administration
- Updated quarterly
- Status field:
  - Materials requested
  - Materials received
  - Administratively closed
  - Appeal under review
  - Decision reached



ISCAP No.	DATE OF REQUEST	Requestor (Last)	Source (Library or Agency)	STATUS
2013-104	7/22/2013	Johnson	Reagan Presidential Library	Materials Received from Agency
2013-105	7/29/2013	Larson	Department of Defense	Materials Requested from Agency
2013-106	8/1/2013	Weber	Department of Defense	Administratively Closed FY 2013
2013-107	8/5/2013	Ravnitzky	Central Intelligence Agency	Materials Received from Agency
2013-108	8/5/2013	Burr	Department of Defense	Materials Received from Agency
2013-109	8/6/2013	Burr	Department of Defense	Materials Requested from Agency
2013-110	8/12/2013	Pesavento	Central Intelligence Agency	Decision Reached FY 2014
2013-111	8/14/2013	Johnson	Department of Defense	Materials Requested from Agency
2013-112	8/14/2013	Vick	Central Intelligence Agency	Administratively Closed FY 2013
2013-113	8/15/2013	Burr	Central Intelligence Agency	Materials Received from Agency
2013-114	8/16/2013	Jones	Central Intelligence Agency	Appeal Under Review by the ISCAP
2013-115	8/21/2013	Rojas	Central Intelligence Agency	Decision Reached FY 2014
2013-116	8/21/2013	Rojas	Department of State	Materials Received from Agency

Links and Contact Information

- ISCAP Appeals Status Log:
  - http://www.archives.gov/declassification/iscap/status-log-description.html
- ISCAP Decisions:
  - http://www.archives.gov/declassification/iscap/decision-table.html
- Contact ISCAP Staff
  - iscap@nara.gov
  - william.carpenter@nara.gov
  - wcarpenter@nara.id.ic.gov
  - william.c.carpenter52.civ@mail.smil.mil
  - 202-357-5466

OPEN HOUSE

Information Security Oversight Office

Protect • Inform • Assess

November 3, 2016 9:30 a.m.–12:30 p.m.

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

Public Interest Declassification Board (PIDB) Overview
Ellen Knight. Senior Program Analyst, ISOO

Public Interest Declassification Board

- Advisory group (most senior-levels of government and private sector)
  - Created to promote "the fullest possible public access to a thorough, accurate, and reliable documentary record of significant … national security decisions and … activities."
  - Advises the President and other executive branch officials on the identification, collection, review for declassification and release of declassified records and materials of archival value.
  - Advises the President and other executive branch officials on policies deriving from the issuance by the President of Executive orders regarding the classification and declassification of national security information.

Enabling Legislation

- Established by the Public Interest Declassification Act of 2000 (Public Law 106-567, Title VII, Dec. 27, 2000, 114 Stat. 2856).
- Modified and extended by:
  - Public Law 113–126- Intelligence Authorization Act for Fiscal year 2014
    - Section 311 extends the Public Interest Declassification Act of 2000 until 2018.
  - Public Law 111–259- Intelligence Authorization Act for Fiscal Year 2010
    - Section 365 improves the review authority of the PIDB.
  - Public Law 112–235 -Public Interest Declassification Board Reauthorization Act of 2012
    - Section 2 extends the Public Interest Declassification Act of 2000 until 2014 and amends the appointments of members.
  - Public Law 110–53- Implementing Recommendations of the 9/11 Commission Act of 2007
    - Section 602(2) of the Act provides the PIDB authority to make reviews and recommendations.
  - Public Law 108–458 -Intelligence Reform and Terrorism Prevention Act of 2004
    - Section 1102 of the Act provides an extension and improvement authorities of the PIDB.

Membership of the PIDB

- Officially composed of nine individuals:
  - Five appointed by the President.
  - Four appointed by Congressional leaders:
    - One each by the Speaker and Minority Leader of the House as well as the Majority and Minority Leaders of the Senate.
- Appointees are U.S. citizens who are preeminent in the fields of history, national security, foreign policy, intelligence policy, social science, law, or archives.
- Director of ISOO serves as Executive Secretary of the PIDB.
  - ISOO staff provides all support for the PIDB's work.

Current Members

- Presidential appointees:
  - Trevor W. Morrison (Chair)
  - James E. Baker
  - Laura A. DeBonis
  - William H. Leary
  - Solomon B. Watson, IV

- Congressional appointees:
  - Sanford J. Ungar, appointed by the Minority Leader of the Senate
  - Kenneth L. Wainstein, appointed by the Majority Leader of the Senate

2007 *Improving Declassification* Report

- 2007 Report focused on improving declassification.
  - Addressed 15 issues and contained 49 recommendations, including creating a National Declassification Center and prioritizing the review of records to focus on "historically significant" records.
  - Several recommendations were later enacted in E.O. 13526, including establishment of the National Declassification Center.

- Presidential tasking:
  - As a result of the 2007 Report, the President tasked the PIDB to "design a more fundamental transformation of the security classification system."
  - Tasking is part of a study undertaken in cooperation with the National Security Advisor .
  - Part of Presidential memorandum entitled Implementation of the Executive Order "Classified National Security Information," (December 29, 2009).

2012 *Transforming the Security Classification System* Report

- 2012 Report focused on transforming the security classification system for the digital age.
  - Addressed 14 recommendations concerning classification, declassification and the use of technology to reform and modernize the system.
  - Primary recommendation for a White House led Steering Committee adopted in 2014.
    - Classification Reform Committee has focused its efforts on piloting technology solutions in support of improved declassification and reforming the treatment of historical nuclear information (Formerly Restricted Data).
    - Both of these stemmed from recommendations made by the PIDB and are now commitments made in the President’s Second Open Government National Action Plan.

2014 *Setting Priorities* Report

- 2014 Report focused on topic-based declassification prioritization.
  - Supplemental Report built on recommendations from earlier 2012 report on *Transforming the Security Classification System.*
  - Involved stakeholders in a process to identify topics for prioritization.
  - Focused on reviewing those topics and records of highest interest first.
  - Six recommendations:
    1. Topic-based declassification should be the normal process rather than the exception.
    2. The National Declassification Center, in consultation with the public and with agencies, should design and implement a process to solicit, evaluate and prioritize standard topics for declassification government-wide.
    3. End pass/fail determinations and identify necessary redactions for topic-based reviews.
    4. The government should require agencies to develop and use new technologies to assist and improve declassification review.
    5. Agencies and the National Declassification Center must improve risk management practices.
    6. Revisions to the current Executive Order are needed to lessen the burden of automatic declassification on agencies in support of topic-based declassification review.

Current PIDB Initiatives

- Continues investigating, soliciting comments, and making recommendations to support 2012 report.
  - Continues the public discussion of the transformation through its blog, *Transforming Classification .*
  - Supports declassification proposals involving high value historical records, including collections at the Presidential Libraries.
- Integrating and using technology in declassification review.
  - Technology study underway that includes founding a working group of agency technologists to understand and make recommendations for technological solutions in support of declassification.
- Assists the White House-led Steering Committee as they lead and manage the implementation of reforms into the next Administration.
  - Next public meeting will be on Thursday, December 8th at the Archives.
  - What transparency/open government initiatives should the next Administration focus on and what changes do we need to the Executive Order?

Web Resources

- Public Interest Declassification Board:
  - http://www.archives.gov/declassification/pidb
- Reports and recommendations:
  - http://www.archives.gov/declassification/pidb/recommendations/
- *Transforming Classification* Blog:
  - http://blogs.archives.gov/transformingclassification/

OPEN HOUSE

Information Security Oversight Office

Protect • Inform • Assess

November 3, 2016 9:30 a.m.–12:30 p.m.

ISOO

INFORMATION SECURITY
OVERSIGHT OFFICE

OPEN HOUSE

Information Security Oversight Office

Protect • Inform • Assess

November 3, 2016 9:30 a.m.–12:30 p.m.

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE

Closing remarks
William Cira, Acting Director, ISOO