ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

Open HOUSE

May 8, 2015 • 9:30 a.m.–4 p.m.

McGowan Theater, National Archives Building
700 Pennsylvania Avenue, NW Washington DC, 20408

www.archives.gov/isoo

NATIONAL
ARCHIVES

Information Security Oversight Office

Protect • Inform • Assess

8 May 2015

Why An Open House?

- Interact
  - Make today the start of something
  - Get (re-) acquainted
- Listen
  - We want to hear from you
- Learn
  - Our updates affect your programs
  - Your 'real world' should guide our actions

ISOO Mission and Vision

Our Mission	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.
Our Vision	• A Government whose information is properly shared, protected, and managed to serve the national interest. • An informed American public that has trust in its Government.

ISOO Values

Our Values	**Integrity, collective expertise, and leadership guide our performance**
	We value our contribution to national security, public trust, & meeting constituent needs
	National Security: We advance national security by ensuring the proper classification, safeguarding, sharing, and declassification of information pertaining to national defense or foreign relations of the United States.
	Public Trust: We strive to uphold the public's confidence in open, effective government by assessing and improving programs intended to protect, share, and release information.
	Constituent Needs: We value the input of our partners and are committed to advising, assisting, and advocating for the American public; federal, state, local, and tribal governments; industry; and private sector entities.

ISOO Goals

1	• Promote programs for protection of classified and controlled unclassified information.
2	• Promote access by ensuring that the systems for declassification and decontrol operate as required.
3	• Reduce classification and control activity to the minimum necessary.
4	• Provide expert advice and guidance to constituents.
5	• Collect, analyze, and report valid information about the status of agency programs.
6	• Maximize ISOO's efficiency and effectiveness.
7	• Invest in our people.

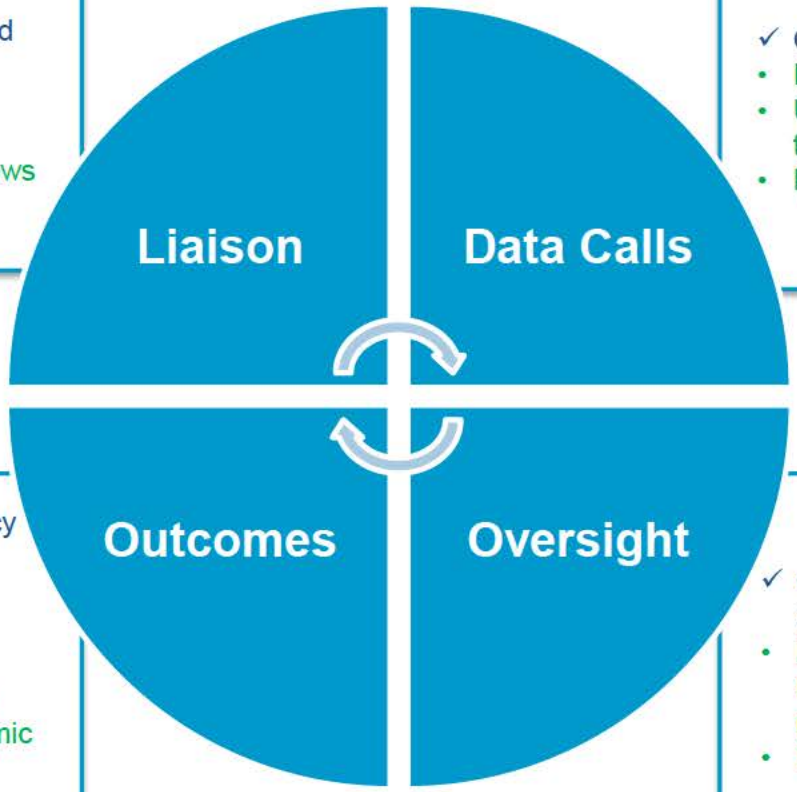
ISOO Liaison and Oversight

- Complete cycle including follow-up
- Focus on integrating liaison with oversight
- New initiatives in green

✓ Continue agency engagement and administrative activities
- Broaden liaisons' knowledge of/interaction with agencies
- Integrate liaison with on-site reviews

✓ Continue current data calls
- Incorporate surveys
- Use self-inspection reports as input to on-site reviews
- Explore use of additional tools

Provide Advance Communications



✓ Prepare Reports to Senior Agency Officials
✓ Provide Input to Annual Report
✓ Provide ISOO Guidance on common issues
- Improve follow up with agencies
- Identify best practices and systemic issues and feed into outreach activities

✓ Continue declassification assessments as configured
- Liaison participates in on-site reviews, attends CUI meetings/appraisals
- Integrate CUI Assessments

CLASSIFICATION MANAGEMENT

Develops security classification policies for classifying, declassifying and safeguarding national security information generated in Government and industry.

Annual Report/Cost Report

Interagency Security Classification Appeal Panel (ISCAP)

Public Interest Declassification Board (PIDB)

Declassification Assessments

ISOO Notices

INFORMATION SECURITY CLASSIFICATION APPEALS PANEL

Established by E.O. 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
  Website for declassified documents

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.

FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW

FIRST REVIEW COMPLETED IN JUNE 2012, NEXT ONE TO BE COMPLETED JUNE 2017

COMPREHENSIVE REVIEW OF AGENCY'S CLASSIFICATION GUIDANCE, PARTICULARLY CLASSIFICATION GUIDES, TO ENSURE THE GUIDANCE REFLECTS CURRENT CIRCUMSTANCES

THE REVIEW SHALL INCLUDE AN EVALUATION OF CLASSIFIED INFORMATION TO DETERMINE IF IT MEETS THE STANDARDS FOR CLASSIFICATION UNDER SECTION 1.4 OF THE ORDER, TAKING INTO ACCOUNT AN UP-TO-DATE ASSESSMENT OF LIKELY DAMAGE.

THE REVIEW SHALL INCLUDE ORIGINAL CLASSIFICATION AUTHORITIES AND AGENCY SUBJECT MATTER EXPERTS TO ENSURE A BROAD RANGE OF PERSPECTIVES.

AGENCY HEADS SHALL PROVIDE A REPORT SUMMARIZING THE RESULTS OF THE REVIEW TO THE DIRECTOR, ISOO, AND SHALL RELEASE AN UNCLASSIFIED VERSION OF THIS REPORT TO THE PUBLIC.

Controlled Unclassified Information

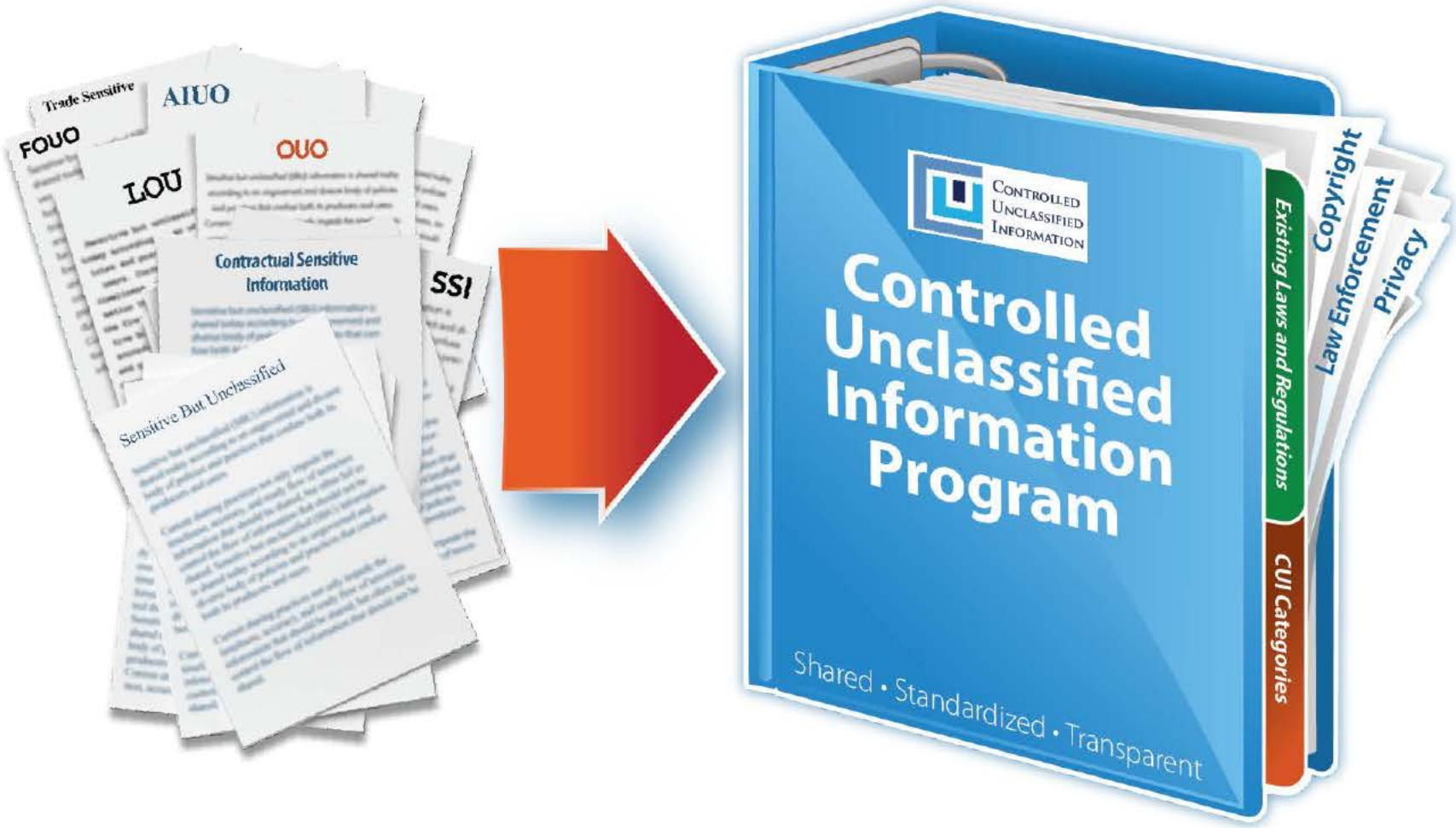
Executive Order 13556

Shared • Standardized • Transparent

CONTROLLED
UNCLASSIFIED
INFORMATION

Information Security Oversight Office (ISOO)

Overview of the CUI Program



Executive Order 13556

- Established CUI Program

- 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**

- 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

Approved CUI Categories

23 Categories		82 Subcategories
Agriculture	Law Enforcement	• Bank Secrecy • DNA • Investigation
Controlled Technical Information	Legal	
Copyright	NATO	
Critical Infrastructure	Nuclear	
Export Control	Patent	
Emergency Management	Privacy	• Financial • Health Information • Personnel
Financial	Proprietary Business	
Foreign Government	Safety Act Information	
Geodetic Product Information	Statistical	• Census • Investment Survey
Immigration	Tax	
Information Systems Vulnerability Information	Transportation	
Intelligence		

Handling CUI

One uniform and consistent policy applied to a defined and organized body of information

Phased Implementation

E.O. 13556 Sec. 5. Implementation (b):

After a review of agency plans, and in consultation with affected agencies and the Office of Management and Budget, the Executive Agent shall establish deadlines for phased implementation by agencies.

Phased Implementation

As of 3/17/15

	Day 0 – Planning	Day 180 – Readiness	Year 1 – Initiation	Year 3-4 – Final
Phases	Identify and initiate planning activities for CUI implementation	Prepare environment and workforce for the CUI transition	Begin implementation of CUI practices Begin Phase Out of obsolete practices	Full Implementation of the CUI program
Key EA Activities	• Publish 32 CFR Part 2002 Rule & Supplemental Guidance (Day 0) • Augment Registry • Provide Awareness Materials & Products • Consult with OMB & Provide Budget Guidance • Review Agency Policies	• Publish CUI Training (Day 180) • Provide Additional Guidance as needed • Establish Schedule for On-site Reviews • Provide Training Support & Consultation	• Oversee Executive Branch Implementation • Resolve Disputes & Complaints • Initiate On-site Reviews	• Oversee Executive Branch Implementation • Collect Reporting Data
Monitor & Report on Phased Implementation				

Key D/A Activities	• **Develop & Publish Policy***
	• Develop Training/Awareness
	• Develop IT Transition Plan
	• Continue Internal Budget Planning
	• Develop Self-Inspection Plan
	• Develop Process to Manage CUI Status Challenges
		• **Assert Physical Safeguarding***
		• **Conduct Training***
		• Initiate Awareness
		• Prepare IT Transition
		• Continue Internal Budget Planning
			• Initiate CUI Implementation
			  • Handle
			  • Recognize
			  • Receive
			• Initiate IT Transition
			• Permit Creation of CUI
			• Initiate Self-Inspection Program
				• Eliminate Old Markings
				• Assure use of only New Markings
				• Complete IT Transition
				• Meet Refresher Training Requirements

IOC

FOC

CONTROLLED UNCLASSIFIED INFORMATION

***Required for IOC**

CUI and IT Implementation

- "This order shall be implemented in a manner consistent with…applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget", Section 6(a)3, Executive Order 13556.

- Future CUI guidance where it addresses IT issues, must be aligned to Federal policies.

NIST Special Publication 800-171


NIST Special Publication 800-171
Final Public Draft

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The final publication of Special Publication 800-171 is targeted for June 2015

Final Public Draft

April 2015

Purpose and Applicability

To provide federal agencies with recommended requirements for protecting the confidentiality of CUI when such information resides in nonfederal information systems and organizations.

The security requirements apply only to components of nonfederal information systems that process, store, or transmit CUI.

CUI Approach for Contractor Environment

Government

E.O. 13556 → Registry → 32 CFR 2002 & Supplemental Guidance → NIST Standards → FAR

Industry

1 Year

Until the formal process of establishing a single FAR clause takes place, the CUI requirements in NIST SP 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.

OPERATIONS & INDUSTRIAL SECURITY

Mission

Evaluate the effectiveness of security classification programs to protect information vital to our national security interests

Oversight & Assessment

Conduct On-Site Reviews
Analyze self-inspection program reporting data

Outreach

Policy Development

Advisory Committees

National Industrial Security Program Policy Advisory Committee (NISPPAC)

State, Local, Tribal and Private Sector Policy Advisory Committee (SLTPSPAC)

Onsite review methods include examination of:

- Program Management
- Classification Practices and Procedures to include document reviews
- Employee Interviews
- Security Education and Training programs for employees
- Security violation handling and other reporting requirements
- Classified Information Systems
- NISP Administration where applicable

OPERATIONS & Industrial Security

Classification Challenges. Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information…..

YEAR	CLASSIFICATION ACTIVITY	CLASSIFICATION CHALLENGES	% OF CHALLENGES VS. CLASS ACTIVITY
FY 2012	95,253,720	402	.0004%
FY 2013	80,183,183	68	.00008%
FY 2014	77,515,636	813	.0010%

OPERATIONS & INDUSTRIAL SECURITY

National Industrial Security Program Policy Advisory Committee (NISPPAC)

Includes Government and industry representatives

Recommends changes in industrial security policy through modifications to Executive Order 12829, its implementing directives, and the National Industrial Security Program Operating Manual

Advises ISOO on all matters concerning the policies of the National Industrial Security Program, and serves as a forum to discuss policy issues in dispute.

OPERATIONS & INDUSTRIAL SECURITY

State, Local, Tribal and Private Sector Policy Advisory Committee (SLTPSPAC)

Includes Federal, State, Local, and Tribal Governments, and Private Sector entities involved in the sharing of classified information

Recommends policies and procedures designed to remove impediments to information sharing with those entities responsible for securing the nation's critical infrastructure and key resources

Promotes consistency in safeguarding classified information

Afternoon Sessions

1:00-1:50	
Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations	McGowan Theater
ISOO Liaison Program Overview/Meet & Greet	Jefferson Room
Public Interest Declassification Board (PIDB) Overview Interagency Security Classification Appeals Panel (ISCAP) Overview	Washington Room
2:00-2:50	
Derivative Classification Program Overview	McGowan Theater
Controlled Unclassified Information Registry	Jefferson Room
National Industrial Security Program (NISP) Overview Self-Inspection Program Execution and Reporting	Washington Room
3:00-3:45	
Panel – Frequently Asked Questions and the Future	McGowan Theater
3:45-4:00	
Closing Remarks	McGowan Theater

Local Restaurants

1. Starbucks
2. Grand Trunk (South Asia
3. Potbelly
4. 701
5. Chop't
6. Plan B Burger Bar
7. Native Food (Vegan)
8. Carmine's (Italian)
9. The Capital Grille

The Café in the National Archives Building at Washington, DC, is open Monday through Friday, 8:00 a.m. to 2:30 p.m. There are also vending machines in the basement, and a small area with seating. It is located on the same level as the McGowan Theater.

Be sure to enter building through the Constitution Ave side of building.

The **70th Anniversary of V-E Day**. The airplanes flying overheard on this day will again celebrate the victory of the allies, and some of the aircraft will be the very same which flew those 70 years ago.

Beginning around noon, 14 formations that comprise the “Arsenal of Democracy” collection aircraft will fly over the Mall at 1,000 feet.