

# Information Security Oversight Office

Protect • Inform • Assess



# An Overview of the Information Security Oversight Office

## Presentation to the Freedom of Information Act Advisory Committee

December 10, 2020

**John Powers**

*Associate Director for Classification Management*

# Information Security Oversight Office

- Created in 1978 under Executive Order 12065
- An organization within the National Archives
  - Policy guidance from the National Security Advisor
  - Report to the Executive for Agency Services
- Organizational Structure
  - Director – Mark Bradley
  - Administrative Staff (3) and Attorney-Advisor
  - Operations Directorate (9)
    - Onsite operations
    - Controlled Unclassified Information Program
    - National Industrial Security Program
    - State, Local, Tribal, and Private Sector Program
  - Classification Management Directorate (5)
    - Declassification Assessments
    - Interagency Security Classification Appeals Panel
    - Public Interest Declassification Board

# ISOO's Authorities and Roles

Primary responsibilities - all are focused on information:

- E.O. 13526, “Classified National Security Information”
- E.O. 12829, as amended, “National Industrial Security Program”
- E.O. 13556, “Controlled Unclassified Information”
- E.O. 13549, “Classified National Security Information Program for State, Local, Tribal and Private Sector Entities”
- E.O. 13587, “Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information”

# ISOO's Purpose

## Mission Statement

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.

## 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.

## Values

Our performance is guided by integrity, collective expertise, and leadership. We value our contribution to national security, public trust, and meeting constituent needs.

# ISOO Primary Responsibilities

- Develop Implementing Directives
  - 32 C.F.R. 2001 – Classified National Security Information
  - 32 C.F.R. 2002 – Controlled Unclassified Information
  - 32 C.F.R. 2003 – Interagency Classification Appeals Panel
  - Binding on the Executive branch
- Provide Instructions and Policy Guidance
  - Maintain Liaison Program with Agencies
  - Security Education and Training
- Conduct Oversight and Inspections
  - Collect Data and Information from Agencies
  - Report on Results
- Act on Complaints, Appeals, and Suggestions
- Serve as spokesperson to Congress, Media, and Public

# Other Responsibilities

- Interagency Security Classification Appeals Panel
  - D/ISOO serves as Executive Secretary
  - ISOO Staff provides all administrative and program support
- National Industrial Security Program Policy Advisory Committee
- State, Local, Tribal, and Private Sector Policy Advisory Committee
- Controlled Unclassified Information Advisory Council
  - NARA (ISOO) serves as the Executive Agent
- Public Interest Declassification Board
  - D/ISOO serves as Executive Secretary
  - ISOO staff provides all administrative and program support

## Classified National Security Information

- ISOO Oversight Role:
  - Onsite inspections and assessments
    - Classification policies and practices
    - Safeguarding policies and practices
    - Declassification policies and practices
  - Collect data and information
    - Agency Fundamental Classification Guidance Reviews
    - Original Classification Authority designations
    - Responses to questions on agency information security programs
  - Publish an Annual Report to the President
    - Typically issued in May or June each year
    - Focused on the deteriorating health of the classification and declassification system



# E.O. 13526

- Classification
  - Section 1 of E.O. 13526
  - Provided detail on classification authority
    - Set standards for classification
    - Established yearly training requirements
    - Listed categories of information that could be classified
    - Set duration for classification and required proper marking/identification
    - Set prohibitions and limitations
    - Established Fundamental Classification Guidance Reviews (FGCR)
      - Designed to ensure guidance is current
      - Required every five-years
- ISOO role in classification
  - Oversight: onsite inspections and required data submissions
  - Collect agency OCA information, FGCR and data for analysis
  - Security Education and Training

## Original Classification vs. Derivative Classification

- **Original Classification:**
  - “An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure”
- **Derivative Classification:**
  - “Incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance”
    - Classification Guides
- **Original Classification Authority**
  - “An individual authorized in writing, either by the President, the Vice President or by agency heads or other officials authorized by the President, to classify information in the first instance”
    - Approve Classification Guides

# E.O. 13526

- Declassification
  - Section 3 of E.O. 13526
  - Specified that *all* information subject to declassification
  - Allowed for the declassification of artifacts
  - Tightened criteria for exempting information
  - Established limits and thresholds for exemptions to auto. Declass.
    - 25, 50, and 75 years
  - Established the National Declassification Center
    - Role of section 3.3(d)(3) – limit unnecessary referrals
- ISOO roles related to declassification
  - Oversight: declassification assessments and required data submissions
  - Issue guidance to improve declassification reviews
  - Conduct training to help agencies
  - Support ISCAP

# The ISCAP

## The Interagency Security Classification Appeals Panel

- 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
    - Declassification Guides
    - Approvals required every five years
  - Decide on mandatory declassification review (MDR) appeals
  - Inform senior agency officials and the public of its decisions
    - Classification challenges
    - MDR Appeals
- Bylaws codified in 32 C.F.R. 2003

## Membership

- Department of Defense
- Department of Justice
- Department of State
- National Archives and Records Administration
- National Security Council
- Office of the Director of National Intelligence
  
- Central Intelligence Agency
  - Temporary Membership in certain instances
  
- Agencies assign staff to serve as Liaisons
  - Perform day-to-day work
  - Participate in bi-monthly meetings
  
- ISOO provides all administrative and program support
  - D/ISOO serves as the Executive Secretary

# ISCAP Activity

## ISCAP Activity 2018-2020

- Declassification Guides – five-year requirement
  - 2020: 1 addendum
  - 2019: 23 guides
  - 2018: started the process
- Appeals
  - 2020: 2 cases
  - 2019: 24 Cases
  - 2018: 37 Cases
- Classification Challenges
  - None
- Backlog of MDR cases awaiting decisions
  - 2020: 1313
  - 2019: 1286
  - 2018: 1217

# ISOO's Annual Report

- Recent reports focused on the need for modernization of information management and information security policies and practices
  - National security imperative
  - Require sustained White House leadership
  - Require significant technology investments
    - Coordinated across agencies
    - Technology-driven changes
  - Require new metrics and cost accounting to improve oversight
- Current challenges
  - Over-classification and information sharing
  - Security education and training has improved
    - Issues of compliance remain
  - Performance management critical element
  - Declassification programs are ill-prepared for the Digital Age

# Public Interest Declassification Board

- Established by Congress
  - Five broad focus functions
    - Improving classification, declassification, and public access to Government information
- Five Reports to the President
  - *Improving Declassification* (2009)
  - *Transforming the Security Classification System* (2012)
  - *Setting Priorities: An Essential Step in Transforming Classification* (2014)
  - *The Importance of Technology in Classification and Declassification* (2016)
  - *A Vision for the Digital Age: Modernization of the U.S. Classification and Declassification System* (2020)
- Five current members
- ISOO provides all administrative and logistical support
  - D/ISOO serves as Executive Secretary



## *A Vision for the Digital Age*

- Immediate Impact
  - Direct the Secretaries of Defense and Energy and DNI to develop a joint plan with the Archivist to modernize classified systems and records management
  - Deploy Technology to support classification and declassification
  - Implement secure communications connectivity between agencies
  - Empower the NDC to implement processes to prioritize declassification
  - Simplify the classification system
  - Develop a new model for measuring classification and declassification
- Strategic Policy Change
  - Designate an Executive Agent and an Executive Committee with the authority to design and implement a new system
  - Organize at the enterprise level, developing a federated system
- Strategic Technology Change
  - Transition to using technology to make classification and declassification more precise

# ISOO and PIDB: Looking to the Future

- ISOO Annual Reports (2017-2018)
  - Need for modernization
  - Need to have technology at center of reform
- ODNI IG FOIA Report (2018)
  - Need for new policies and processes
  - Need for ODNI to integrate and collaborate IC-wide
  - Need for technology and secure communications
- PIDB Report (2020)
  - Need for Cabinet-Level agency head to serve as Executive Agent
  - Need White House to drive reform and change culture
  - Need for technology investment and use

# The Last Slide

## Information – Seek, Learn, Participate, Contact

### ISOO:

- Website: [www.archives.gov/isoo](http://www.archives.gov/isoo)
- The ISOO Overview Blog: <https://isoo-overview.blogs.archives.gov/>
- The CUI Program Blog: <https://isoo.blogs.archives.gov/>
- E-mail: [isoo@nara.gov](mailto:isoo@nara.gov) and [cui@nara.gov](mailto:cui@nara.gov)

### PIDB:

- Website: [www.archives.gov/declassification/pidb](http://www.archives.gov/declassification/pidb)
- Transforming Classification Blog:  
<https://transforming-classification.blogs.archives.gov/>
- Email: [pidb@nara.gov](mailto:pidb@nara.gov)

John Powers

Associate Director

Information Security Oversight Office

[john.powers@nara.gov](mailto:john.powers@nara.gov)