# 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

Welcome
David Ferriero, Archivist of the United States

# 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

ISOO Overview—Current Efforts
Open House Overview
William Cira, Acting Director, ISOO

# Information Security Oversight Office

- Created in 1978 under Executive Order 12065
- Oversee the Executive Branch's system for classifying, safeguarding, and declassifying classified information
- An organization within the National Archives
- Receive policy guidance from the National Security Advisor
- Primary responsibilities.
  - 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 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.<br>• 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

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

# ISOO Oversight Authority

- ISOO's oversight authority comes from the Presidential executive order: "Director, ISOO shall have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports and information and other cooperation that may be necessary."

- Onsite review methods include examination of:
  - Program Management
  - Classification Practices and Procedures to include document reviews
  - Training programs for employees
  - Internal Inspections
  - Security violation handling
  - Classified Information Systems

# CLASSIFICATION MANAGEMENT

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

Interagency Security Classification Appeal Panel (ISCAP)

Public Interest Declassification Board (PIDB)

Declassification Assessments

Annual Report/Cost Report

ISOO Notices

# OPERATIONS & INDUSTRIAL SECURITY

Evaluate the effectiveness of the security classification programs established by Government and industry to protect information vital to our national security interests.

National Industrial Security Program Policy Advisory Committee (NISPPAC)

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

Conduct On-Site Reviews of Executive Branch Agency classified information programs

# CUI EXECUTIVE AGENT

- Issuance of implementing directives and guidance.
- Approval of categories and subcategories.
- Maintain a registry of all approved categories and subcategories, markings, safeguarding, dissemination and decontrol.
- Oversight of department and agency implementation.
- Establish a phased implementation.
- Publish an annual report for the first five years.

# 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

Self-Inspection Program Execution and Reporting
On-site Review & Follow up
Robert Skwirot, Senior Program Analyst, ISOO


SELF-INSPECTIONS

# What is the purpose of self-inspections?

# Why the detailed reporting?

## Self-Inspection Program Requirements of E.O. 13526

- The senior agency official establish and maintain an on-going self-inspection program
- Regular reviews of representative samples of the agency's original and derivative classification actions
- Authorize appropriate agency officials to correct misclassification actions
- Report annually to the Director of ISOO on the agency's self-inspection program

# Self-Inspection Program Requirements of 32 CFR Part 2001

- SAO responsible for directing and administering
- SAO designates personnel to carry out responsibility
- Program to be structured to provide SAO with
  - information necessary to assess the effectiveness of the CNSI program
    - within individual activities and
    - the agency as a whole

# Self-Inspection Program Requirements of 32 CFR Part 2001

- Evaluate adherence to the principles and requirements of the Order and Directive
- Evaluate effectiveness of agency programs covering
  - Original Classification
  - Derivative Classification
  - Declassification
  - Safeguarding
  - Security Violations
  - Education and Training
  - Management and Oversight

# Self-Inspection Program Requirements of 32 CFR Part 2001

- Review of Classification Actions
  - Regular reviews of representative samples of the agency's original and derivative actions
  - Encompass all activities that generate classified information
  - Include a sample of varying types of classified information (in document and electronic format)
  - Proportionally sufficient to enable a credible assessment of agency's classified product
  - Personnel who conduct are knowledgeable of classification and marking requirements and have access to pertinent classification guides.
  - SAO authorize appropriate agency officials to correct misclassification

# Self-Inspection Program Requirements of 32 CFR Part 2001

- Frequency:  At least annually, with SAO setting frequency based on program needs and degree of classification activity
- Coverage:  SAO establishes self-inspection coverage requirements based on program or policy needs
- Reporting, Internal:
  - SAO sets format for documenting
  - Security education and training should address underlying causes of findings and concerns of a systemic nature
- Reporting, External
  - SAO reports annually to the Director of ISOO

# SELF-INSPECTION PROGRAM

## What should self-inspections accomplish?

- Help the Senior Agency Official and Security Personnel better manage the classified national security information program.
- Identify the strengths and weaknesses of the CNSI program so that steps can be taken to address any shortcomings.

# SELF-INSPECTION PROGRAM

## What should be included in the annual self-inspection report to ISOO?

- Information that shows that self-inspections are indeed accomplishing those things.
- That self-inspections are helping the SAO and security personnel manage the CNSI program,
- That self-inspections are identifying the strengths and weaknesses of the CNSI program, and
- That actions are being taken to address shortcomings.

# SELF-INSPECTION PROGRAM

Enclosure 2

## AGENCY ANNUAL SELF-INSPECTION PROGRAM DATA: FY 2016

**(Submissions must be unclassified.)**

| **PART A: Identifying Information** | |
|---|---|
| 1. Enter the agency name. | 1. |
| 2. Enter the date of this report. | 2. |
| 3. Enter the name, title, address, phone, fax, and e-mail address of the **Senior Agency Official** (SAO) (as defined in E.O. 13526, section 5.4(d)) responsible for this report. | 3. |
| 4. Enter the name, title, phone, fax, and e-mail address of the **individual or office** responsible for conducting self-inspections and reporting findings. | 4. |
| 5. Enter the name, title, phone, fax, and e-mail address for the **point-of-contact** responsible for answering questions regarding this report. | 5. |
| **PART B: Classified National Security Information (CNSI) Program Profile Information** | |
| 6. Has your agency been designated/delegated as an original classification authority (OCA)? | 6. ◯ Yes ◯ No |
| 7. Does your agency perform original classification activity? | 7. ◯ Yes ◯ No |
| 8. Does your agency perform derivative classification activity? | 8. ◯ Yes ◯ No |
| 9. Does your agency have an approved declassification guide and declassify CNSI? | 9. ◯ Yes ◯ No |
| **PART C: Self-Inspection Program Activity: Number of Self-Inspections Conducted** | |
| In FY 2014 and prior years, this information was reported on Standard Form 311, "Agency Security Classification Management Program Data." | |

# SELF-INSPECTION PROGRAM

**PART D: Description of the Program**

A description of the agency's self-inspection program to include activities assessed, program areas covered, and methodology utilized. The description must demonstrate how the self-inspection program provides the SAO with information necessary to assess the effectiveness of the CNSI program within individual agency activities and the agency as a whole.

Responsibility

**PART E: A summary of the findings of your agency's self-inspection program**

The **summary** should present specific, concise findings from your self-inspection program for each of the required program areas below. It is not a description of the requirements of the agency's CNSI program. Rather, the summary outlines the essential self-inspection findings based on the compilation and/or distillation of the information contained in the agency's internal self-inspection reports, checklists, etc. In large agencies where findings are drawn from multiple agency offices and activities, the findings that are reported here may be the most significant or most frequently occurring.

45. Original Classification:

**PART F: An assessment of the findings of your agency's self-inspection program**

The **assessment** discerns what the findings mean. The assessment is an evaluation of the state of each element of your agency's CNSI program based on an analysis of the specific, concise findings of the self-inspection program. It reports what you have determined the findings indicate about the state of your agency's CNSI program.

The assessment should inform the SAO and other decision makers of significant issues that impact the CNSI program. It should be used to determine how security programs can be improved, whether the agency regulation or other policies and procedures must be updated, and if necessary resources are committed to the effective implementation of the CNSI program. The assessment should report trends that were identified during the reporting period across the agency or in particular activities, as well as trends detected by making comparisons with earlier reporting periods. It can be used to support assertions about the successes and strengths of an agency's program.

52. Original Classification:

# SELF-INSPECTION PROGRAM

| PART G: Focus Questions |
| --- |
| Answer the questions below. If the response identifies a deficiency, it should be explained in Part D, Summary of Findings, under the relevant program area, and should be addressed in Part H, Corrective Actions. |
| Training for Original Classification Authorities |

| PART H: Findings of the Annual Review of Agency's Original and Derivative Classification Actions |
| --- |
| In this section provide specific information with regard to the findings of the annual review of the agency's original and derivative classification actions to include the volume of classified materials reviewed and the number and type of discrepancies identified. |
| 94. Indicate the volume of classified materials reviewed during the annual review of agency's original and derivative |

| PART I: Corrective Actions |
| --- |
| 96. Describe actions that have been taken or are planned to correct identified program deficiencies, marking discrepancies, or misclassification actions, and to deter their reoccurrence. |

# SELF-INSPECTION PROGRAM

| PART J: Best Practices |
| --- |
| Best practices are those actions or activities that make your self-inspection program and/or CNSI program more effective or efficient. They set your program apart through innovation or by exceeding the minimum program requirements. These are practices that may be utilized or emulated by other agencies. |
| 97. Describe best practices that were identified during the self-inspection. |
| |

| PART K: Explanatory Comments |
| --- |
| *98. Use this space to elaborate on any section of this form. If more space is needed, provide as an attachment to this form. Provide explanations for any significant changes in trends/numbers from the previous year's report.* |
| |

# Strengths and Weaknesses of Self-Inspection Reports


ON-SITE REVIEWS

## Authority for On-Site Reviews:

E.O. 13526, section 5.2(b)(4) gives ISOO
"the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports and information and other cooperation that may be necessary to fulfill its responsibilities."

# ON-SITE REVIEWS

## Process:

- Agency POCs are notified by their ISOO liaison of the agency's selection for a review and of proposed dates, which are subject to confirmation.
- A formal notification letter is sent by the Director of ISOO to the senior agency official. (45 to 60 days prior to the review)
- The review is coordinated by the ISOO review team lead with personnel identified by the agency. The team lead provides additional details of coverage and requirements.
- To save time on-site, the agency is asked to provide information and program documentation two weeks prior to the review.
- Full-program reviews generally are a full week, on-site.
- In-Brief and out-brief with the senior agency official
- Written report from the Director of ISOO to the senior agency official
- Agency responds within 90 days with steps to correct findings

# ON-SITE REVIEWS

## Coverage:

- Program management,
- Classification management,
- Security education and training,
- Self inspections,
- Security violations,
- Safeguarding,
- Classified information systems,
- Industrial security, and
- Review of classified documents.

# ON-SITE REVIEWS

## Methodology:

- Examination of program documentation;
- Review of classified documents generated by the agency, both originally and derivatively;
- Interviews with personnel
  - who are responsible for implementing the classified national security information (CNSI) program and
  - who generate or handle classified information, to include original classifiers, derivative classifiers, and users of classified information
- Examination of areas where classified information is stored and/or processed.

## Types of On-Site Reviews

Full-Program On-Site Reviews

Follow-Up On-Site Reviews

# Full-Program On-Site Reviews

- Purpose: Review of classified national security information program (CNSI), including information systems, to determine if the requirements of E.O. 13526 and 32 CFR Part 2001 are being met
- Scope: Broad CNSI program, including program management, classification management, security education and training, self-inspections, safeguarding, information systems security, security violations, and industrial security, along with a review of 200 classified documents created by the agency in the two years prior to the review.
- Time on-site: One week

# Follow-Up On-Site Reviews

(Generally conducted two years after the initial review)

- Purpose: Verify/validate agency corrective actions to address observations and recommendations from previous ISOO on-site review
- Scope: Limited to those program elements for which corrective actions were needed after the previous ISOO on-site review. Follow-up document reviews sample 50 documents created by the agency in the year prior to the review.
- Time on-site: Two days

# Coverage Specifics

**Program Management:**

- The agency's organization for security, including security responsibilities of personnel involved in the implementation of the information security program;
- the agency's policies for rating personnel whose duties significantly involve the designation and/or management of classified information; and
- the support for the CNSI program from senior management.

**Classification Management:**

- Classification guides,
- Appropriateness of classification, and
- Classification challenges.

# Coverage Specifics

**Security Education and Training:**

- The scope, content, and tracking of security indoctrination, refresher, and termination briefings, as well as training for original classification authorities, persons who apply derivative classification markings, other specialized training, and other measures used to promote security awareness.
- Among the related issues that we will cover are whether waivers have been granted if individuals have not received OCA or derivative classification training and whether findings from self-inspections and trends identified in incidents and violations are incorporated into refresher training.

**Self-Inspections:**

- The agency's policies and procedures for internal inspections;
- A review of self-inspection reports from the past two years.
- This element will also validate the agency's most recent self-inspection report to ISOO.

# Coverage Specifics

**Security Violations:**

- The agency's policies and procedures to identify, investigate, and address security violations and infractions;
- Records of security infractions and violations for the past two years;
- Trends and how they are identified and tracked.

**Safeguarding:**

- The agency's policies and procedures for safeguarding CNSI.
- Includes observation of areas where CNSI is stored and/or processed, checks of security equipment, and verification of the use of standard forms and labels.

**Classified Information Systems:** The agency's policies and implementation procedures as they relate to the confidentiality, integrity, and availability of information processed on all automated information systems used to collect, create, process, transmit, store, and disseminate classified information by, or on behalf of the agency.

# Coverage Specifics

**Industrial Security:**

- The agency's policies and implementation of its program for industrial security;

**Document Review:**

- Approximately 200 documents that were generated, originally or derivatively, by the agency during the two years prior to the review.
- Representative of the agency's classification actions with regard to offices that generate the documents and to the types and classification levels of documents that are created.
- It is very important that the documents be identified and collected prior to the ISOO visit. It is nearly impossible to obtain documents if the agency is searching for the materials when we are on site.
- If documents can be accessed or made available via a JWICS or SIPRNet connection or by another means, all or part of the document review can be conducted during the weeks prior to the review.

# ON-SITE REVIEWS

**What does ISOO consider a successful on-site review?**

# 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

National Industrial Security Program (NISP)
Kathleen Branch

# National Industrial Security Program (NISP)

Single, cohesive, integrated program to ensure the protection of classified information in the hands of industry

- Established by E.O. 12829
- Implemented through 32 CFR 2004, NISP Directive
- ISOO implements and monitors
- Policy direction from the NSC
- 5 CSAs:  DoD, DOE, NRC, ODNI, DHS
- DoD is Executive Agent
  - Issues NISPOM for industry
  - Provides oversight services for executive branch agencies that are not one of the CSAs

# National Industrial Security Program Policy Advisory Committee (NISPPAC)

Addresses policy issues and other NISP matters of interest and concern

- ISOO Director chairs
- 16 government and 8 industry members
  - Subject to FACA
  - Meeting notices in the Federal Register
  - Meets 3x/year
- Working groups established as needed
  - Personnel security
  - Assessment and authorization (information systems in industry)
  - Insider threat
  - NISPOM rewrite

NEXT MEETING: Thursday, November 10, 2016, 10 am to noon

# 32 CFR 2004

- Current version issued in 2010
  - Updated original 2006 version
  - Incorporated requirements and timelines for NIDs
- Establishes responsibilities for NISP agencies
  - ISOO
  - Executive Agent
  - CSAs
  - GCAs

# 32 CFR 2004 Revision

- Adds insider threat responsibilities and requirements for NISP agencies (E.O. 13587)
- Recognizes DHS as a CSA (E.O. 13691)
- Recognizes ODNI as a CSA (IRTPA)
- Fills gaps in guidance for NISP agencies to align with NISPOM provisions for contractors
  - Consistent standards for determinations of contractor eligibility for access to classified information
  - Consistent standards to determine and mitigate FOCI
  - Contract security classification responsibilities
  - Oversight of contractor industrial security programs
  - Terminology and definitions to accommodate all 5 CSAs
- STATUS: OMB clearing the ISOO responses to the inter-agency comments. Once done, will issue as proposed rule and request public comments.

# 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