Information Security Oversight Office

Protect • Inform • Assess

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE

Greg Pannoni

May 2016

National Industrial Security Program (NISP)

"…single, integrated, cohesive industrial security program…"

Goal: eliminate redundant, overlapping, or unnecessary requirements that impeded national security interests.

- Established by EO 12829
- Implementation:
  - 32 CFR 2004 for Government Agencies
  - NISPOM for Contractors

- ISOO responsible for:
  - Implementing and monitoring the NISP
  - Chairing the NISPPAC

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

NISP Update

EO 12829 amended in Feb 2015


FEDERAL REGISTER

EO 13691, "Promoting Private Sector Cybersecurity Information Sharing"

- Establishes DHS as a NISP CSA – for cybersecurity critical infrastructure
- Clarifies ODNI as a NISP CSA vice the CIA

Now 5 CSAs:

DoD, the NISP Executive Agent

DOE

NRC

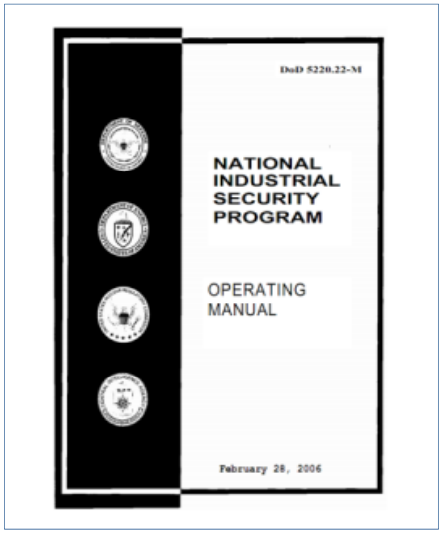
ODNI

DHS

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

Update: NISPOM

Two revisions underway:


DoD 5220.22-M

NATIONAL INDUSTRIAL SECURITY PROGRAM

OPERATING MANUAL

February 28, 2006

Change 2 to the 2006 version of the NISPOM:

Incorporates **insider threat provisions** for industry from EO 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"

Complete revision to replace the 2006 version of the NISPOM

- CSAs and NISPPAC working with DoD
- Reflects up-to-date NISP operations

NISPOM Change 2

Insider Threat Program

- Establish and Maintain Insider Threat program
  - Designate Insider Threat Senior Official
  - Gather, Integrate and Report relevant and available information indicative of a potential or actual insider threat
  - Insider Threat Training
    - Insider Threat Program Official
    - All cleared employees
  - User activities on classified systems are subject to monitoring

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

NISPOM Change 2

- **Contractor Reviews**
  - More guidance on content, scope, and mgmt. support, including an annual certification by a senior mgmt. official.
  - Formal report for CSA review.

- CSA guidance will be based on guidance for Federal ISs

- **New Appendix D:** NISPOM Supplement: will cancel 1995 NISPOM Supplement 1
  - No gap in guidance, since DoD will not publish NISPOM change #2 until DoD SAP volumes are published.

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

Update: 32 CFR 2004

ISOO responsible for the NISP Implementing Directive

- Last revised in 2010 to clarify the NID process

- Complete revision underway with the CSAs
  - Incorporates NISP insider threat responsibilities for CSAs and GCAs
  - Fills a national-level policy gap for Executive Branch Agencies
    - Expands the current regulation and clarifies responsibilities for:
      - Sharing information
      - Determining eligibility for access to classified information for companies and their employees
      - FOCI and NIDs

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

NISPPAC

Membership comprised of the CSAs, other Executive Branch Agencies, industry representatives

- Provides advice to the Chair on NISP policy matters
- Industry members nominated by their peers
- Subject to FACA, Freedom of Information Act, Government Sunshine Act

  - 3 meetings a year
  - Meeting notices in the Federal Register

  - Summer meeting:
    - Monday, June 6 in Nashville, TN
    - During the Annual NCMS Seminar
    - Gaylord Opryland Hotel
      2:00 pm in Delta Ballroom D

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

NISPPAC INDUSTRY MEMBERS

- **Tony Ingenito** — **Northrop Grumman**
  Term: 2012-2016 (Industry Lead) — e-mail: Tony.Ingenito@ngc.com
- **J.C Dodson** — **BAE Systems**
  Term: 2012-2016 — e-mail: jeffrey.dodson@baesystems.com
- **William Davidson** — **Keypoint Government Services**
  Term: 2013-2017 — e-mail: william.davidson@keypoint.us.com
- **Phil Robinson** — **Squadron Defense Group**
  Term: 2013-2017 — e-mail: phillip.robinson@squadrondefense.com
- **Martin Strones** — **Strones Enterprises**
  Term: 2014- 2018 — e-mail: mstrones@gmail.com
- **Michelle Sutphin** — **BAE Systems**
  Term: 2014-2018 — e-mail: michelle.sutphin@baesystems.com
- **Dennis Keith** — **Harris Corporation**
  Term: 2015-2019 — e-mail: Dkeith@harris.com
- **Quinton Wilkes** — **L-3 Communications Corporation**
  Term: 2015-2019 — e-mail: Quinton.Wilkes@L-3com.com

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

NISPPAC Working Groups

Opportunity for NISPPAC members to address specific areas of interest

Standing Working Groups

- Personnel Security Clearance
- Contractor Information Systems

Ad Hoc

- NISPOM Rewrite
- SAP
- Insider Threat

CUI Program Update

- 32CFR2002 (CUI Implementing Regulation) is scheduled to be released June, 2016.
  - Projected Effective Date: August, 2016

- On the effective date (or Day Zero), agencies will begin implementation activities.
  - Modification to agency policy, training, physical safeguarding, system configuration, self-inspection programs, and contracts (agreements)

- August 2017, one year from effective date, CUI Federal Acquisition Regulation will be published.

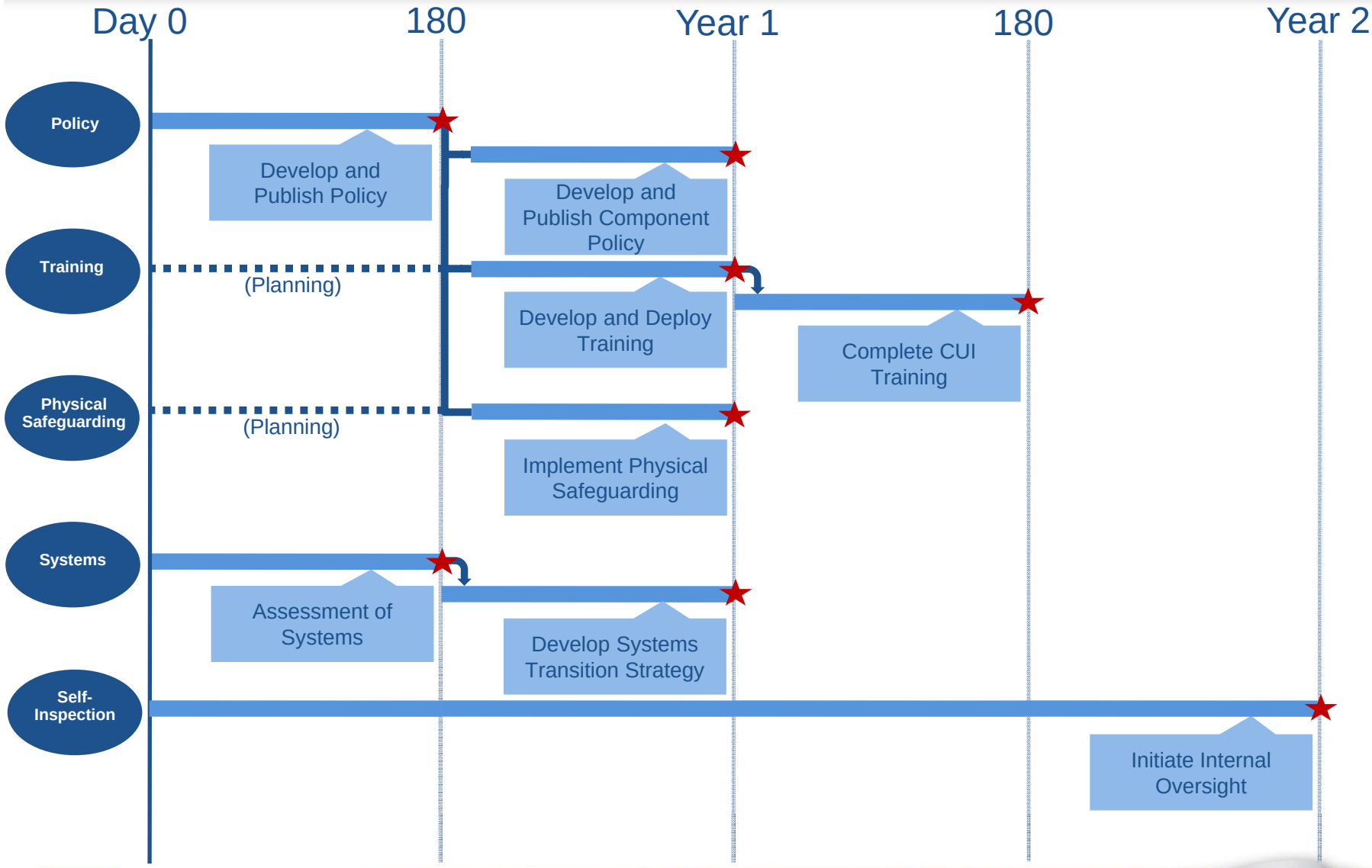
32 CFR 2002 (June 2016)

- Implements the CUI Program
  - Establishes policy for designating, handling, and decontrolling information that qualifies as CUI

- Describes, defines, and provides guidance on the minimum protections for CUI
  - Physical and Electronic Environments
  - Destruction
  - Marking
  - Sharing

- Emphasizes unique protections described in law, regulation, and/or Government-wide policies (authorities)
  - These protections must continue as described in the underlying authorities.

Implementation Activities within Executive Branch



CUI Approach for Contractor Environment

Government

E.O. 13556

Registry

32 CFR 2002

NIST SP 800-171

FAR

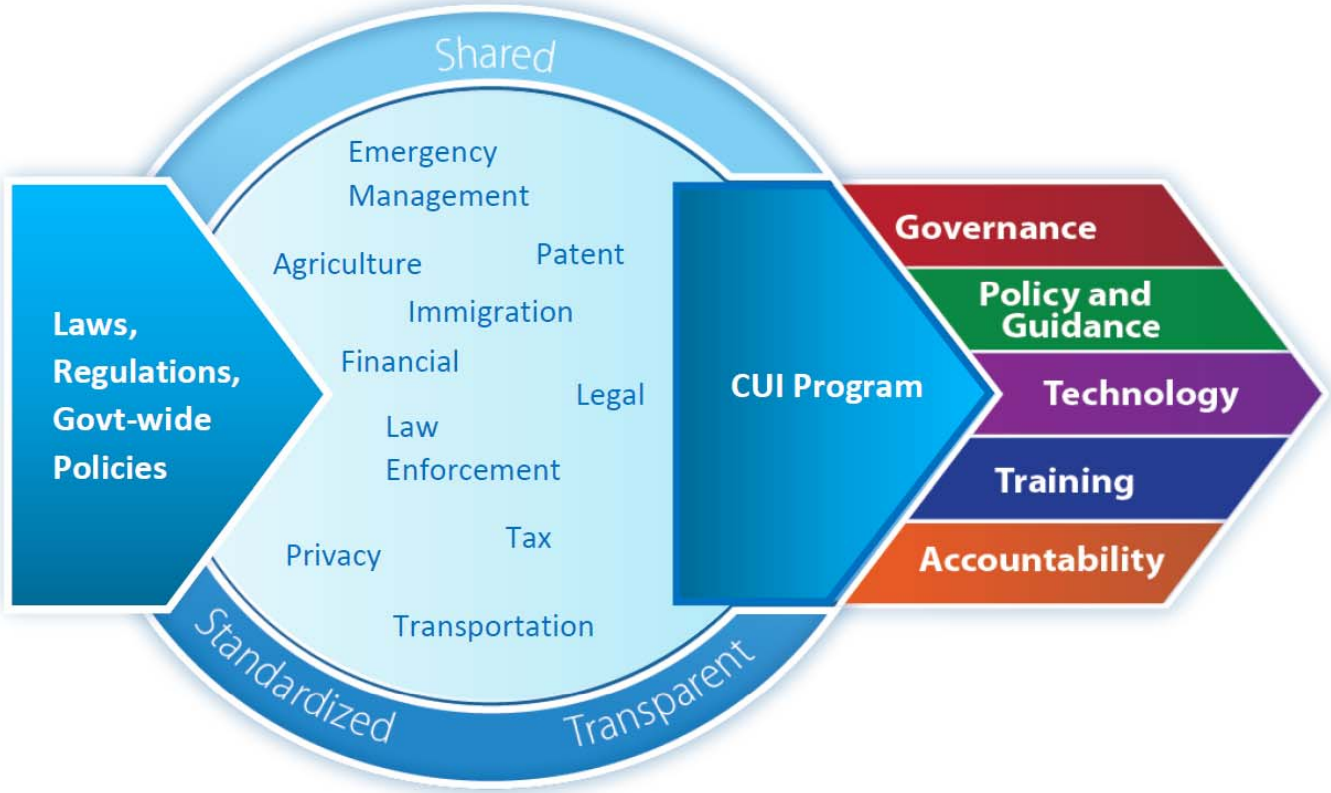
Industry

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.

The Department of Defense has revised its DFARS to reference the NIST SP 800-171.

Submit any questions to: CUI@NARA.GOV



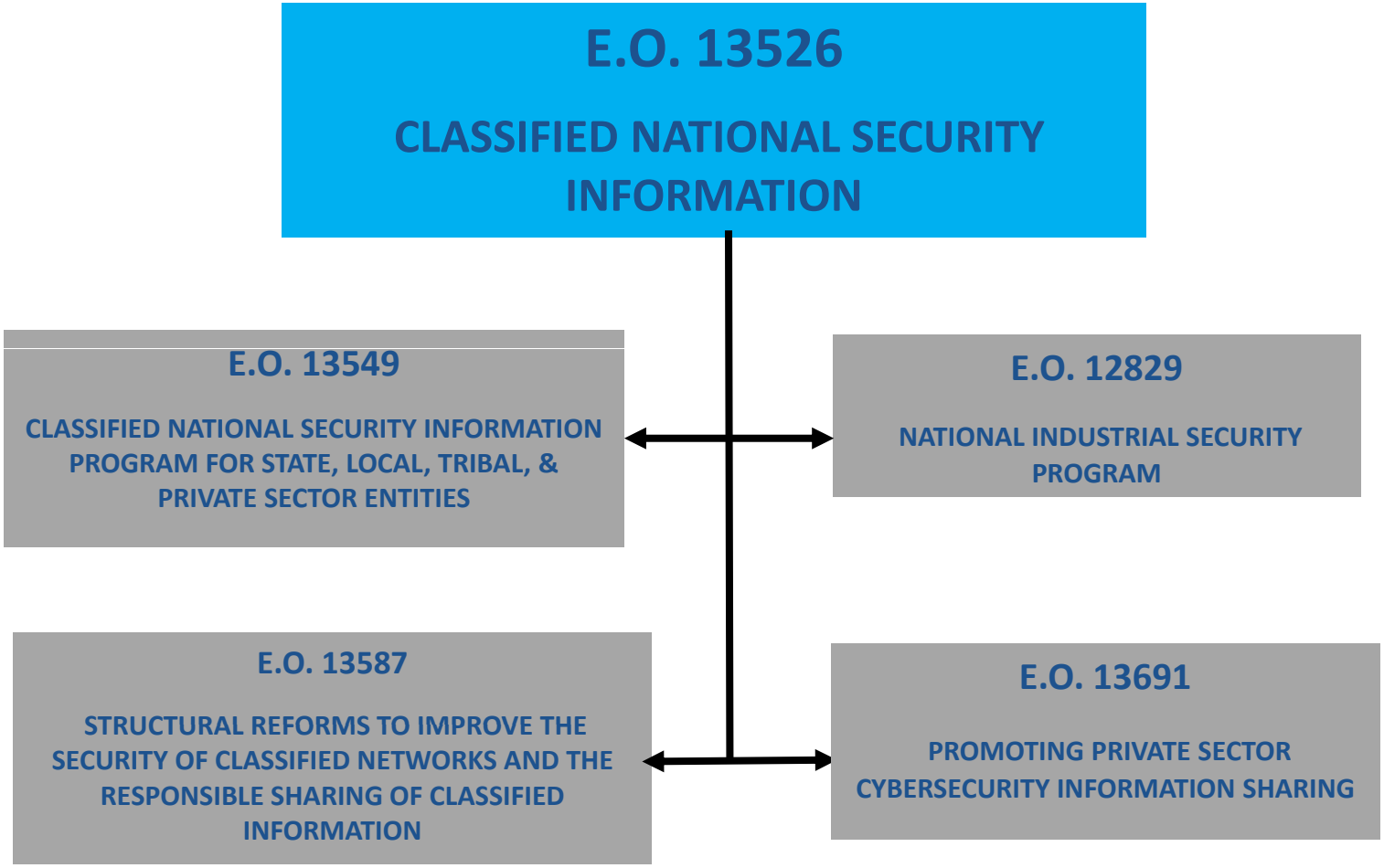
Web Resources

- ISOO Web Page:
  - http://www.archives.gov/isoo/
- ISOO Policy Documents:
  - E.O. 12829:
    - http://www.archives.gov/isoo/policy-documents
  - Implementing Directive (32 C.F.R. Part 2004):
    - http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.html
- NISP and NISPPAC sections
  - Member listings
  - Charter and Bylaws
  - Minutes of NISPPAC meetings

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

BACKUP

NISP POLICY RELATIONSHIPS



E.O. 13526

Classified National Security Information

(12/29/2009)

E.O. 13587

Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

(10/7/2011)

E.O. 12829

National Industrial Security Program

(1/8/1993)

E.O. 13549

Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities

(8/18/2010)

E.O. 13556

Controlled Unclassified Information

(11/4/2010)

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

NISPOM Change 2

Insider Threat Training

- Considered appropriate by the CSA
  - Personnel with insider threat program responsibilities
    - Counterintelligence and security fundamentals
    - Procedures for conducting insider threat response actions
    - Applicable laws related to use (or misuse of records and data)
  - All other cleared personnel
    - Insider threat awareness training
- Training required before access to classified information
- Establish and maintain a record of all cleared employees who have completed the initial and annual training

NISPOM Change 2

Information Systems Security

- ISSM role includes insider threat awareness
- User activities on contractor's classified systems are subject to monitoring
  - Banners on all classified information systems (ISs)
    - Activity on classified network is subject to monitoring
    - Could be used in criminal, security or administrative actions
- Security awareness training for all users (initial and refresher) (chp 3)
- CSA guidance will be based on guidance for Federal ISs
  - Terminology updates to synchronize to NIST 800-37
    - e.g., Assessment and Authorization instead of Certification and Accreditation

ISOO INFORMATION SECURITY OVERSIGHT OFFICE