National Industrial Security Program (NISP)

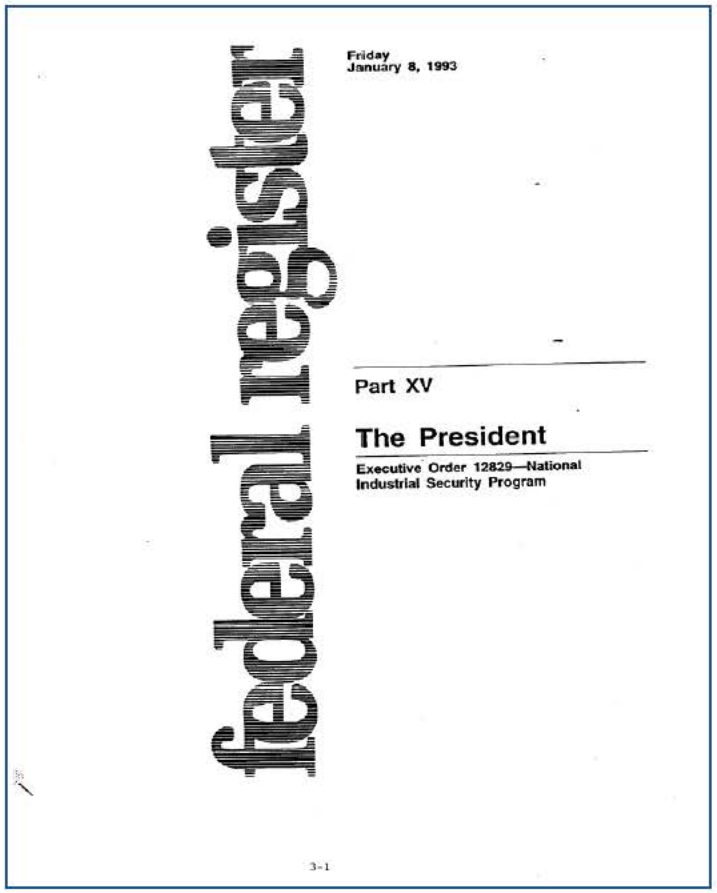
Information Security Oversight Office

Protect • Inform • Assess

May 8, 2015

National Industrial Security Program (NISP)

Basis in Executive Order 12829, as amended


federal register

Friday
January 8, 1993

Part XV

The President

Executive Order 12829—National Industrial Security Program

3-1

- The NISP shall serve as an:
  - Single
  - Integrated
  - Cohesive

Industrial Security Program

- Applies to all executive branch departments and agencies that have contracts with private sector entities that require access to classified information

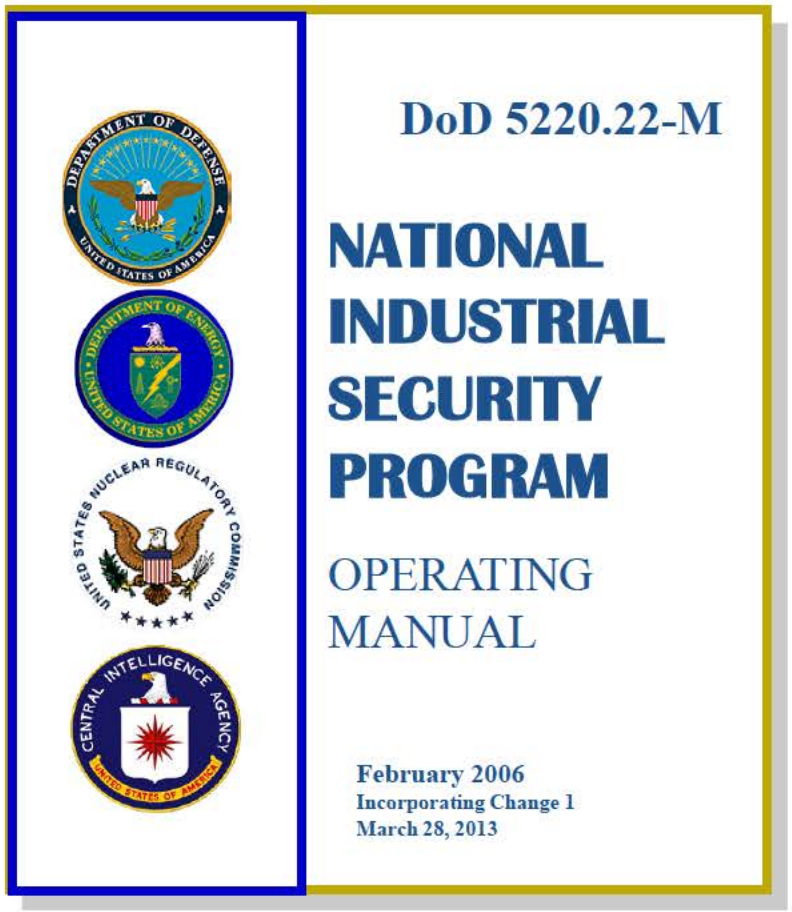
Security Management in the NISP

Joint responsibility

Government

Industry

NATIONAL INDUSTRIAL SECURITY PROGRAM



Department of Defense :

- Executive Agent for NISP
- Cognizant Security Agency (CSA) for DoD & Non CSA Agencies
- Executes oversight through Defense Security Service

Department of Energy and Nuclear Regulatory Commission

- Authority over information under Atomic Energy Act of 1954

Office of Director of National Intelligence

- Authority over Sensitive Compartmented information

Department of Homeland Security

- Authority over Critical Infrastructure Protection per E.O. 13691

Responsibilities of ISOO Director

- Ensure NISP is operated as a single, integrated program, across the Executive Branch, and that agencies adhere to NISP principles
- Ensure each Contractor's NISP implementation is overseen by a single Cognizant Security Authority(CSA), based on a preponderance of classified contracts per agreement by the CSA's
- Ensure Agencies contracting for classified work have included the Security Requirements Clause (52.204-2) from the FAR
- Ensure Agencies where DoD serves as CSA have entered into agreements to establish their responsibilities on behalf of those Agency heads
- Chairs the NISP Policy Advisory Committee (NISPPAC)

CSA Responsibilities

The CSAs:

- **Conduct oversight inspections of contractor security programs and provide other support necessary for contractor compliance with NISPOM**
- **Ensure contractors are protecting classified information as required**
- **Provide training to ensure industry understands its responsibility to protect classified information**
- **Validate contractor need for a classified contract, and establish system for providing security clearances to contractor personnel**
- **Maintain a system of eligibility and access determinations of contractor personnel**

Agency Head Responsibilities

Heads of agencies that issue contracts requiring industry to have access to classified information will:

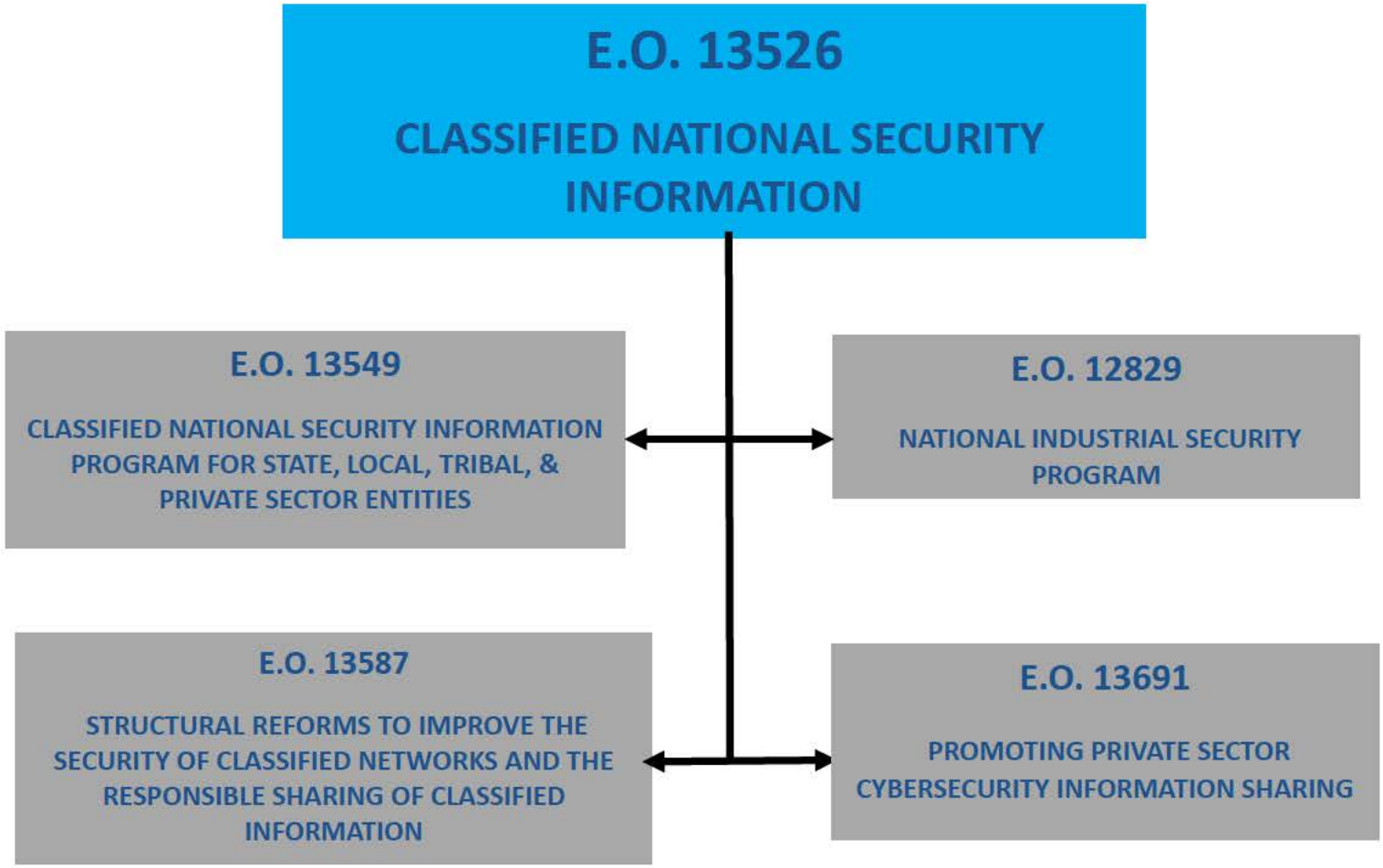
- Designate a Senior Agency Official to administer NISP compliance
- Issue agency implementing regulations and guidance consistent with the NISP E.O., Directive and the NISPOM
- Ensure personnel with NISP responsibilities receive appropriate training
- Take corrective action(s) when violations of E.O., directive or NISPOM occur
- Account for annual costs associated with agency implementation of of the NISP, and report costs to ISOO
- Ensure contractors report insider threat activity to the appropriate CSA and GCA
- Incorporate DD-254 and FAR requirements into contracts.

NISP Contracting Considerations

Security requirements are addressed through a Contract Security Classification Specification (DD-254) and specific contract clauses.

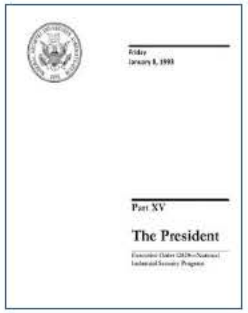
- **Contractor must have a facility security clearance (FCL) to the level of classified information being accessed (Confidential, Secret, Top Secret).**
- **Must have authorized safeguarding capability if classified storage is a contractual requirement.**
- **Federal Acquisition Regulations(FAR) dictate contract requirements and performance**
  - **Agency specific FAR supplements can impact contract requirements**
- **Issues regarding classified information transmission, dissemination and storage should be resolved between Government Contracting Activity (GCA) and Contractor prior to commencing contract activities.**
- **GCA requirements are passed from prime contractor to sub-contractors**

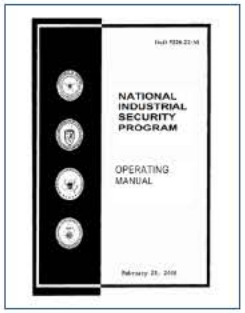
NISP POLICY RELATIONSHIPS



Policy and Direction

Recommends changes to policies reflected in:





Integrates the protection of classified information by industry required under:

E. O. 13549, Classified National Security Information Program for State, Local, Tribal, & Private Sector Entities

E.O. 13587, Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

E.O. 13691, Promoting Private Sector Cybersecurity Information Sharing

NISP Policy Advisory Committee (NISPPAC)

- **Membership**
  - Director ISOO – Chairman
  - Representatives of Government agencies (15 members)
  - Nongovernmental (Industry) representatives (8 members)
- **Functions – Advise the Chairman:**
  - On all matters concerning the policies of the NISP
  - Serves as a forum to discuss policy issues in dispute
- **Authority**
  - E.O. 12829 as amended, *National Industrial Security Program*
  - Subject to Federal Advisory Committee Act (FACA), The Freedom of Information Act (FOIA), and The Government in the Sunshine Act

NISPPAC Government Representatives

Agency	
Information Security Oversight Office	Department of Homeland Security
Central Intelligence Agency	Department of Justice
Defense Security Service	Department of the Navy
Department of the Air Force	Department of State
Department of the Army	National Aeronautics and Space Administration
Department of Commerce	National Security Agency
Department of Defense	Nuclear Regulatory Commission
Department of Energy	Office of the Director of National Intelligence

NISPPAC Industry Members

Members	Company	Term Expires
Rick Graham	Huntington Ingalls Industries	2015
Steve Kipp	L3 Communications	2015
J.C. Dodson	BAE Systems	2016
Tony Ingenito	Northrop Grumman Corp.	2016
Bill Davidson	KeyPoint Government Solutions	2017
Phil Robinson	CGI Federal	2017
Michelle Sutphin	American Systems Corp.	2018
Martin Strones	Strones Enterprises	2018

NISPPAC Working Groups

Permanent Working Groups

- **The Certification and Accreditation (C&A) Working Group**
  - Addresses issues related to the processing of classified information on information systems, and analyzes metrics pertinent to the end-to-end timeliness of the C&A process.
- **The Personnel Security Clearance (PCL) Working Group**
  - Analyzes metrics and makes recommendations to improve the timeliness of the end-to-end clearance Processes.
- **The Policy Integration Working Group (PIWG)**
  - Addresses industry concerns relating to the impacts of government policy that is developed outside of NISP framework
- **E.O. 13587 Working Group**
  - Addresses insider threat and cybersecurity issues as they relate to their implementation by the Cognizant Security Authorities , NISP signatory agencies, and contractors under the NISP

NISPPAC Working Groups

NISPPAC Ad Hoc working groups are established to review specific issues and prepare recommendations for formal NISPPAC decisions.

- NISPOM Rewrite Working Group (12 meetings)
- Threat Information Working Group
- Special Access Programs Working Group
- Small and Middle-Sized company Issues Working Group
- Risk Management Framework Working Group
- Controlled Unclassified Information Working Group
- Foreign Ownership, Control , and influence Working Group

NISPPAC WORKING GROUP ACCOMPLISHMENTS

- Developed NISP implementing directive guidance on National Interest Determinations (NIDS)
- Facilitated Government and Industry collaboration on changes to NISP Operating Manual (NISPOM), through Conforming Changes 1 and 2 and NISPOM rewrite
- Introduced concept for current electronic facilities clearance (e-FCL) system
- Continuing reporting process metrics to NISPPAC for:
  - Certification and Accreditation of Information Systems
  - Personnel Security Clearance processes and timeliness
- Improved interaction, coordination, and cooperation on NISP issue mitigation
- Changes to 32 CFR part 2004 , NISP Implementation Directive, to include Insider Threat Program implementation requirements

Insider Threat and NISP Policy

ISOO implements and monitors and ensures that each Cognizant Security Agency (CSA):

- Issues directions to contractors under their cognizance consistent with the NISPOM 's CSA- specific insider threat guidance
- Shares relevant insider threat information with each other and that they meet reporting requirements
- Conducts ongoing analysis and adjudication of adverse or relevant information about the personal behaviors and activities of contractor employees
- Provides contractors with access to data relevant to insider threat program activities and a designated means to report such activities

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

Questions?