CONTACT INFORMATION

THE INFORMATION SECURITY OVERSIGHT OFFICE

Director, Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, NW, Room 100
Washington, DC 20408 | (202) 357-5250
www.archives.gov/isoo | E-mail: isoo@nara.gov

NISP

www.archives.gov/isoo/oversight-groups/nisp/index.html | E-mail: nisp@nara.gov

NISPPAC

http://www.archives.gov/isoo/oversight-groups/nisppac/ | E-mail: nisppac@nara.gov

DEFENSE SECURITY SERVICE (DSS)

Customer Service | 1-888-282-7682
http://www.dss.mil | E-mail: occ.cust.serv@dss.mil

GOVERNMENT & INDUSTRY MEMBERS

For information on the Government and industry representatives, please visit the NISPPAC website at:
http://www.archives.gov/isoo/oversight-groups/nisppac/membership.html

700 Pennsylvania Avenue, NW
Room 100
Washington, DC 20408
Phone: 202.357.5250
Fax: 202.357.5907
isoo@nara.gov

NISP

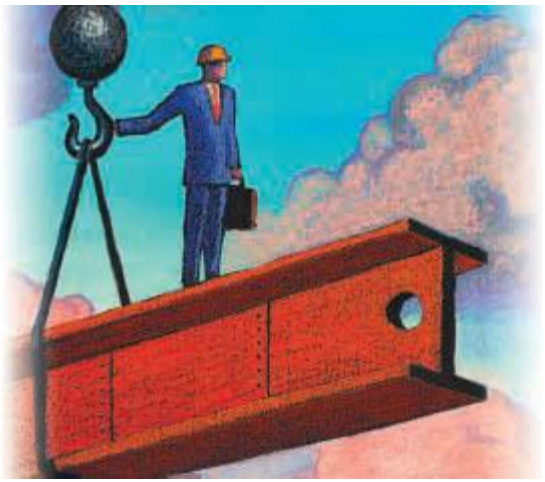
NISP

In January 1993, the National Industrial Security Program (NISP) was established by Executive Order 12829, as amended. The goal of the NISP is the safeguard classified information in the possession of Government contractors, licensees, or grantees in the most efficient and cost effective manner possible.

The NISP applies to all executive branch agencies. The major signatories to the Program are the Department of Energy, the Nuclear Regulatory Commission, the Department of Defense (DOD), and the Central Intelligence Agency.

Consistent with the goal of achieving greater uniformity in security requirements for classified contracts, the four major tenets of the NISP are:

- Achieving uniformity in security procedures.
- Implementing the reciprocity principle in security procedures, particularly with regard to facility and personnel clearances.
- Eliminating duplicative or unnecessary requirements.
- Achieving reductions in security costs.



Policy and Operational Oversight

Information Security Oversight Office— Executive Order 12829, as amended, requires the Information Security Oversight Office (ISOO) to exercise policy oversight on behalf of the National Security Council (NSC). ISOO responsibilities include implementing and monitoring the NISP and overseeing agency, contractor, licensee, and grantee actions to ensure that they comply with Executive Order 12829, as amended. ISOO also reviews all agency implementing regulations, internal rules, or guidelines, and conducts on-site reviews of the implementation of the NISP by each agency, contractor, licensee, and grantee that has access to or stores classified information. Additionally, ISOO reports annually to the President on the NISP. ISOO is also responsible for overseeing the Government-wide security classification program established under Executive Order 13526, "Classified National Security Information". In addition to reporting to the President annually on the status of this program, ISOO performs similar functions to those noted for the NISP. ISOO also recommends policy changes to the security classification system to the President through the NSC.

Secretary of Defense— The NISP assigns operational oversight to the Secretary of Defense, who acts as Executive Agent of the NISP, and has final responsibility for issuing and maintaining the National Industrial Security Program Operating Manual (NISPOM). As the Executive Agent, the Secretary of Defense also provides information on the implementation of the NISP within industry.

Defense Security Service— The Director of the Defense Security Service (DSS) administers the NISP on behalf of the Secretary of Defense and its user agencies. DSS adjudicates OPM personnel security investigations to determine an individual's suitability for access to classified information for a sensitive position within DOD including DOD cleared contractor facilities.

NISPPAC

Executive Order 12829, as amended, also established the National Industrial Security Program Policy Advisory Committee (NISPPAC). The NISPPAC represents a true partnership between Government and industry in policy making. The NISPPAC, with representation from 16 Government and 8 industry members, advises the Director of ISOO (who serves as its Chair) on all matters concerning the policies of the NISP, including recommending changes to those policies. It serves as a forum for discussing policy issues in dispute. In keeping with its oversight responsibilities, ISOO continues to evaluate the effectiveness of the NISP. The NISPPAC has formed working groups to resolve specific issues that arise in the NISP, such as contractor Personnel Security Clearances (PCL); Foreign, Ownership, Control or Influence (FOCI); and the Certification and Accreditation of Information Systems (C&A).

The NISPPAC meets at a minimum of twice a year and its meetings are open to the public. The NISPPAC is administered through the Federal Advisory Committee Act (FACA), its charter, bylaws, as well as reports on committee activities are posted online at the NISPPAC website at:

http://www.archives.gov/isoo/oversight-groups/nisppac/