## CONTACT INFORMATION

### THE INFORMATION SECURITY OVERSIGHT OFFICE

Director
National Archives and Records Administration Building
700 Pennsylvania Avenue, N.W., Room 100
Washington, D.C. 20408 | (202) 219-5250
www.archives.gov/isoo | Email: isoo@nara.gov

### CENTRAL INTELLIGENCE AGENCY (CIA)

Director of Security | Washington, D.C. 20505
(703) 482-9006

### DEPARTMENT OF ENERGY (DOE)

Director, Office of Security
1000 Independence Avenue SW | Mail Stop: SO-1
Washington, D.C. 20585 | (202) 586-3345

### NUCLEAR REGULATORY COMMISSION (NRC)

Director of Facilities and Security
Mail Stop-T7D57 | Washington, D.C. 20555
(301) 415-8080 | Email: tom2@nrc.gov

### THE OFFICE OF THE SECRETARY OF DEFENSE

Director of Industrial Security | OASD (C3I)/ODASD (S&IO)
Room 1E765, 6000 Defense, Pentagon
Washington, DC 20301 | (703) 695-9468

### DEFENSE SECURITY SERVICE

Deputy Director for Industrial Security Program
1340 Braddock Place | Alexandria, VA 22314-1651
(703) 325-5282 | Email: ronald.iverson@mail.dss.mil

### INDUSTRY

For information on the industry representatives, please contact ISOO at the e-mail address or telephone number mentioned above.

INFORMATION SECURITY OVERSIGHT OFFICE

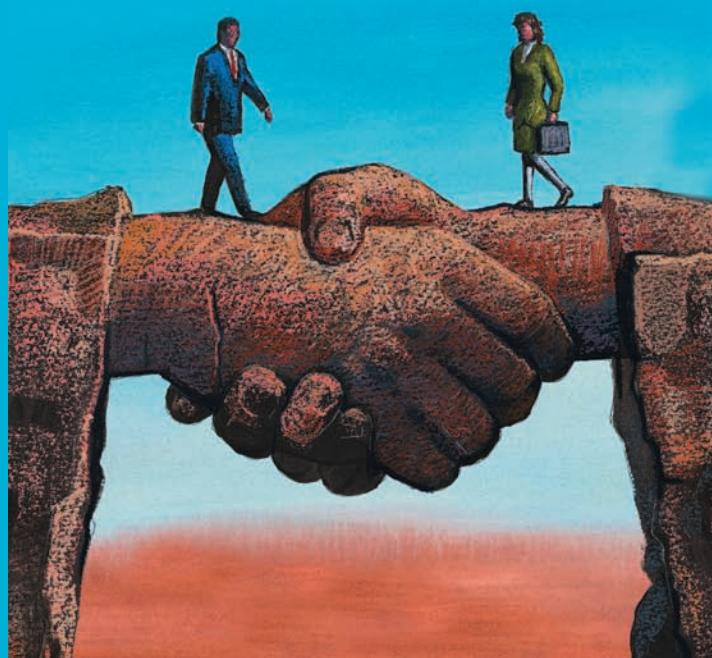
E PLURIBUS UNUM

700 Pennsylvania Avenue, NW
Washington, DC 20408

# NISP

## THE NATIONAL INDUSTRIAL SECURITY PROGRAM

*"Working Together to Protect Classified Information and Preserve our Nation's Economic and Technological Interests."*



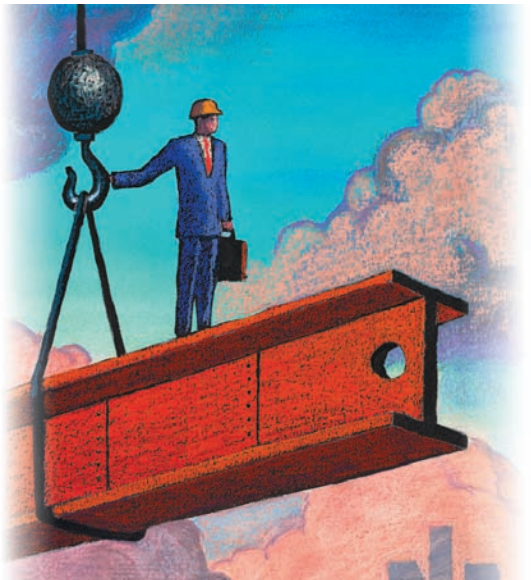
## NISP

In January 1993, the National Industrial Security Program (NISP) was established in Executive Order 12829. The goal of the NISP is to 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 departments and 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, particularly agency inspections.
- Achieving reductions in security costs.



## Policy and Operational Oversight

Information Security Oversight Office—Executive Order 12829 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. 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 12958, "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.

**a single, integrated, cohesive system**

Secretary of Defense—The NISP assigns operational oversight to the Secretary of Defense, who acts as the 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 user agencies. DSS also conducts personal security investigations used by DOD adjudicative facilities to determine an individual's access to classified information for a sensitive position within DOD including DOD cleared contractor facilities.

## NISPPAC

Executive Order 12829 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 Government and industry, advises the ISOO Director, 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.

The NISPPAC meets twice a year and the meetings are open to the public.

## Monitorship

In keeping with its oversight responsibilities, ISOO continues to evaluate the effectiveness of the NISP. In the past, this has been accomplished by conducting surveys with contractors and agencies. In Fiscal Year 1996, ISOO surveyed NISP participants in the Boston, Massachusetts area, and in Fiscal Year 1998, ISOO expanded the focus of its evaluations to include contractors in the Southwest and Western regions, as well as contractors in the Greater Washington, DC area. Future surveys are planned. Click on the "National Industrial Security Program" under Programs and Groups at *www.archives.gov/isoo*.