

NISP

THE NATIONAL INDUSTRIAL SECURITY PROGRAM

*“Working Together to Protect Classified Information and
Preserve our Nation’s Economic and Technological Interests.”*



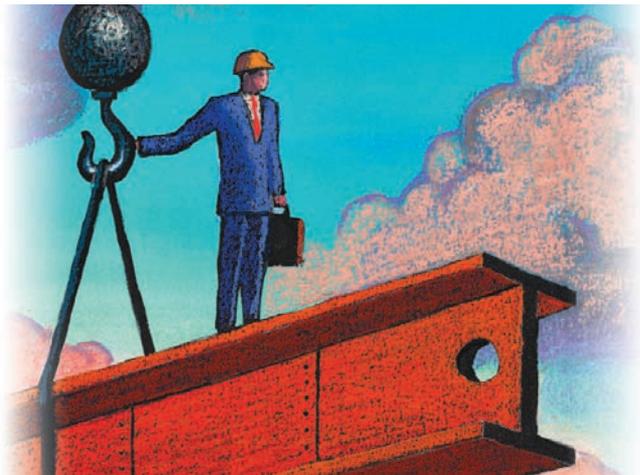
The NISP

Executive Order 12829, “The National Industrial Security Program” (the “NISP”), was established to safeguard classified information held by contractors, licensees, and grantees of the United States Government in a cost effective and efficient manner. The Order was signed by President Bush in January of 1993.

Redundant, overlapping, or unnecessary requirements impede the technological and economic interests of the U.S Government. Executive Order 12829 calls for a single, integrated, cohesive system for safeguarding classified information held by industry. 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.

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, and the Central Intelligence Agency.



Responsible Parties

The 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's responsibilities include implementing and monitoring the NISP and overseeing agency, contractor, licensee, and grantee actions in order to ensure that they comply with Executive Order 12829. ISOO also reviews all agency implementing regulations, internal rules or guidelines, as well as conducting 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 concerning the implementation of 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 listed above 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 the Executive Agent for the NISP, and has final responsibility for issuing and maintaining the National Industrial Security Program Operating Manual (NISPOM). The NISPOM gives practical application to the objectives of the NISP by serving as the single regulatory standard for the NISP. It is a living document constantly being reviewed and updated to fit the changing landscape of industrial security. As the Executive Agent, the Secretary of Defense also provides cost information on the implementation of the NISP.



NISP

Defense Security Service

The Director of the Defense Security Service (DSS) administers the NISP on behalf of the Secretary of Defense and user agencies. In conjunction with these responsibilities, DSS is responsible for inspecting and monitoring the contractors, licensees, and grantees that require access to classified information. Specific DSS actions include clearing approximately 800,000 industry personnel under the NISP on behalf of the Secretary of Defense and 21 other government agencies; ensuring that facilities are eligible to receive classified information; and making certain that contractors have security systems in place to protect the classified information with which they have been entrusted.

A copy of the NISPOM and all of its amendments can be found at www.dss.mil

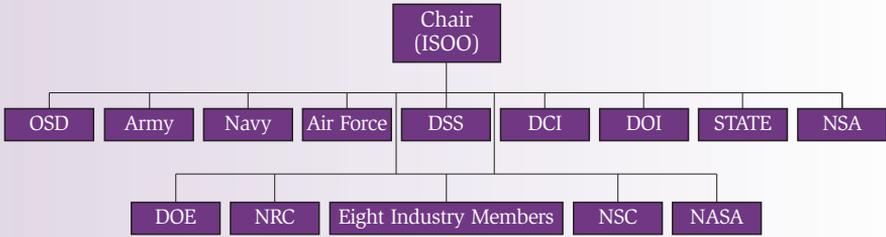
The NISPPAC

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. The NISPPAC also serves as a forum for discussing policy issues in dispute.

The Director of ISOO appoints the members of the NISPPAC. The members of the NISPPAC include 14 representatives from executive branch agencies (including the Chair) and eight representatives from industry. The NISPPAC meets twice a year and the meetings are open to the public.



Organizational Chart of the NISPPAC



NISPPAC Membership

(as of May 1, 2002)

Government Members

- Department of the Air Force
- Department of the Army
- Central Intelligence Agency
- Department of Defense
- Defense Security Service
- Department of Energy
- Department of Justice
- National Aeronautics and Space Administration
- National Security Agency
- Department of the Navy
- Nuclear Regulatory Commission
- Department of State

Industry Members

- Arcadia Group Worldwide, Inc.
- Buckels Security Management Solutions
- The Boeing Company
- Lockheed Martin Corporation
- Science Applications International Corporation
- Washington Group International Government
- MCA Engineers, Inc.
- Northrop Grumman Corporation



Monitoring the NISP

In keeping with its oversight responsibilities under E.O. 12829, ISOO continues to evaluate the effectiveness of the NISP. In the past, this has been accomplished by conducting surveys of contractors and agencies. In Fiscal Year 1996, ISOO surveyed NISP participants in the Boston, MA area. During Fiscal Year 1998, ISOO expanded the focus of its evaluations to include contractors in the Southwest and Western regions of the United States, as well as contractors in the Greater Washington, DC area. The results of this survey were published in *The ISOO Second Report on Selected Aspects of the NISP* which can be obtained by contacting ISOO at (202) 219-5250.

Findings

In its second report of the NISP, ISOO reported progress and areas for improvement. The *Second Report* revealed that there is greater awareness and uniformity in security procedures, increased reciprocal acceptance of personnel and facility security clearances, and increased reciprocal acceptance of agency inspections. All of these achievements helped to reduce security costs.

Notwithstanding these accomplishments, the report indicates areas of concern. They include: (1) the lack of specificity in the NISPOM in regard to procedural matters; (2) Cognizant Security Agencies (CSA) requiring different clearance request forms; (3) the impasse between the Department of Energy and the Department of Defense regarding reciprocal agreements for access and safeguarding Secret Restricted Data; and (4) the diminishing presence and accessibility of the DSS.

a single, integrated,
cohesive s



ISOO is considering ways to address these areas of concern through the Executive Agent and the NISPPAC. In addition, ISOO is preparing to conduct a new and expanded survey of industry in the summer/fall of 2002 to assess the current needs of the NISP.

What is the Future of the NISP?

It is important to remember that the NISP is not a static program. It is constantly changing to meet the needs of the industrial security community. To meet these needs:

- ISOO is increasing its monitorship of the NISP;
- The Executive Agent continues to assess the NISPOM for relevant updates; and,
- The NISPPAC is seeking opinions and ideas from a greater portion of the NISP participants.

Together, industry and Government, are working to meet the goals of E.O. 12829 and to define the future of industrial security for the United States.



NISP

NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) 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, D.C. 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.

