



Department of Defense INSTRUCTION

NUMBER 5220.22

March 18, 2011

Incorporating Change 1, Effective May 1, 2018

USD(I)

SUBJECT: National Industrial Security Program (NISP)

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive (DoDD) 5220.22 (Reference (a)) as a DoD Instruction in accordance with the authority in DoDD 5143.01 (Reference (b)).

b. Establishes policy and assigns responsibilities for administration of the NISP in accordance with Executive Orders 10865 and 12829 (References (c) and (d)) to ensure that classified information disclosed to industry is properly safeguarded.

2. APPLICABILITY. This Instruction:

a. Applies to OSD, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the DoD (hereafter referred to collectively as the "DoD Components").

b. Does not apply to the standards and criteria for determining security eligibility for contractor personnel requiring access to classified information, which are governed by DoDD 5220.6 (Reference (e)).

3. POLICY. It is DoD policy that:

a. The Secretary of Defense, designated as the Executive Agent for the NISP by Reference (d), may prescribe such specific requirements, restrictions, and other safeguards as considered necessary to protect classified information that may be disclosed, or has been disclosed, to current, prospective, or former contractors, licensees, or grantees of U.S. agencies.

b. The Secretary of Defense is authorized by Reference (d) to enter into agreements with any other Executive Branch department or agency to provide industrial security services required for safeguarding classified information disclosed to industry by these departments or agencies. Such departments and agencies, together with the DoD Components, are hereafter referred to collectively as Government Contracting Activities (GCAs).

c. The DoD shall set forth policies, practices, and procedures for the GCAs to follow for the effective protection of classified information provided to industry, including foreign government information that the U.S. Government is obligated to protect in the interest of national security.

4. RESPONSIBILITIES. See Enclosure 2.

5. RELEASABILITY. ~~UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>. Cleared for public release. This instruction is available on the Directives Division Website at <http://www.esd.whs.mil/DD/>.~~

6. EFFECTIVE DATE. This Instruction is effective ~~upon its publication to the DoD Issuances Website. March 18, 2011.~~



Michael G. Vickers
Acting Under Secretary of Defense for
Intelligence

Enclosures

1. References
 2. Responsibilities
- Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5220.22, "National Industrial Security Program," September 27, 2004 (hereby cancelled)
- (b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)), "~~November 23, 2005~~ *October 24, 2014, as amended*
- (c) Executive Order 10865, "Safeguarding Classified Information Within Industry," February 20, 1960, as amended by Executive Order 10909, January 17, 1961
- (d) Executive Order 12829, "National Industrial Security Program," January 6, 1993
- (e) DoD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program," January 2, 1992, *as amended*
- (f) DoD 5220.22-R, "Industrial Security Regulation," December 4, 1985
- (g) DoD Instruction 5025.01, "DoD Directives Program," ~~October 28, 2007~~ *August 1, 2016, as amended*
- (h) DoD Manual 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, *as amended*
- (i) Subpart 4.4 of the Federal Acquisition Regulation, "Safeguarding Classified Information within Industry," current edition

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), in addition to the responsibilities in section 4 of this enclosure, shall:

a. Oversee policy and management of the NISP; direct, administer, and oversee the NISP to ensure that the program is efficient and consistent.

b. Develop and approve changes to DoD 5220.22-R (Reference (f)) in coordination with the DoD Components, in consultation with those Federal agencies with whom the DoD has entered into agreements to provide industrial security services, and in accordance with DoD Instruction 5025.01 (Reference (g)).

c. Develop and approve changes to DoD Manual 5220.22-M (Reference (h), hereafter referred to as the "NISP Operating Manual (NISPOM)),” which sets national standards for the protection of classified information disclosed to industry, in coordination with the DoD Components, and in accordance with Reference (g). As required by Reference (d), obtain concurrence from the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission, and the Director of National Intelligence for such changes.

d. Consult with the NISP Policy Advisory Committee and non-DoD GCAs on all proposed changes to NISP policy.

e. Ensure that appropriate background investigations and security eligibility determinations are provided for contractor personnel requiring access to classified information as established in Reference (e).

2. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). The Director, DSS, under the authority, direction, and control of the USD(I), shall:

a. Administer the NISP as a separate program element on behalf of the GCAs, to include security oversight as the cognizant security office for cleared companies requiring access to classified information for legitimate U.S. Government requirements. DSS is relieved of this oversight function for DoD Special Access Programs when a carve-out provision is approved by the Secretary of Defense or the Deputy Secretary of Defense.

b. Maintain a complete program of certification, accreditation, and oversight of contractor information systems used to process and store classified information.

c. Propose appropriate changes to Reference (f) and the NISPOM to maintain these publications on a current and effective basis and forward to the USD(I) for approval in accordance with Reference (g).

d. Prepare, coordinate, and, after USD(I) approval, publish industrial security letters to provide clarification, interpretation, and guidance to cleared companies and GCAs in carrying out their responsibilities under the NISP and to provide other security-related implementation guidelines.

e. Budget, fund, and administer the NISP.

f. Provide appropriate security education, training, and awareness to industrial and GCA personnel.

g. Decide eligibility for access to classified information by cleared company personnel under DSS cognizance in accordance with Reference (e).

h. Maintain a record of eligibility determinations for cleared company personnel requiring access to classified information who are under DSS cognizance in the DoD system of records for such determinations.

i. Establish and maintain a system for timely and effective communication with NISP contractors and GCAs.

j. Consult with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) or DoD Components, as appropriate, when there is a question as to whether there is a legitimate U.S. Government requirement for contractors or contractor personnel to have access to classified information.

3. USD(AT&L). The USD(AT&L), in addition to the responsibilities in section 4 of this enclosure, shall:

a. Establish acquisition policy, procedures, and guidance, in coordination with the USD(I), that facilitate DoD Component compliance with DoD NISP policies, when classified information is disclosed to contractors in the Defense Industrial Base (DIB).

b. Ensure DoD Components establish and maintain record of a current and legitimate need for access to classified information by DIB companies and personnel.

c. Advise the USD(I) on the development and implementation of NISP policies.

4. HEADS OF THE OSD AND DoD COMPONENTS. The Heads of the OSD and DoD Components shall review all contracts before contract award to decide if releasing classified information is necessary for contract performance. If contract performance is found to require access to classified information, the Heads of the OSD and DoD Components shall:

- a. Include the “Security Requirements” clause in the contract as required by Reference (f) and subpart 4.4 of the Federal Acquisition Regulation (Reference (i)).
- b. Provide security classification guidance to contractors.
- c. Comply with the requirements of Reference (f).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

DIB	Defense Industrial Base
DoDD	DoD Directive
DSS	Director, Defense Security Service
GCA	Government Contracting Activities
NISP	National Industrial Security Program
NISPOM	NISP Operating Manual
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence