DEPARTMENT OF THE NAVY
U.S. NAVAL SUPPORT ACTIVITY NAPLES ITALY
PSC 817 BOX 1
FPO AE 09622-0001

NAVSUPPACTNAPLESINST 5531.1 CH-1
N19
17 Oct 22

NAVSUPPACT NAPLES INSTRUCTION 5531.1 CHANGE TRANSMITTAL 1

From: Commanding Officer, U.S. Naval Support Activity, Naples, Italy

Subj: INDUSTRIAL SECURITY PROGRAM

Encl: (1) Revised Enclosure (2)

1. Purpose. To promulgate change transmittal 1 to subject instruction, reporting changes to page five of the basic instruction to reflect the Defense Information Security System, and changes to Enclosure (2) to remove all references to Joint Personnel Adjudication System.

2. Action

a. Page 5, paragraph 4e(9): Change "Joint Personnel Adjudication System" into "Defense Information System for Security".

b. Replace Enclosure (2) of the basic instruction with revised Enclosure (2) of this change transmittal.

3. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the Department of the Navy Assistant for Administration, Directives and Records Management Division portal page at: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager or the OPNAV Records Management Program (DNS-16).

4. Review and Effective Date. Per OPNAVINST 5215.17A, NAVSUPPACT Naples will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years unless revised or cancelled in the interim and will be reissued by the 10-year anniversary date if it still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

STEWART.JAMES.W.1160963766
Digitally signed by STEWART.JAMES.W.1160963766
Date: 2022.10.17 11:52:36 +02'00'

J. W. STEWART

Releasability and distribution:
NAVSUPPACTNAPLESINST 5216.4DD
Lists: I through IV
Electronic via NAVSUPPACT Naples web site:
https://cnreurafcent.navy.afpims.mil/Installations/NSA-Naples/About/Installation-Guide/Department-Directory/N1-Administration-Department/Instructions/

DEPARTMENT OF THE NAVY
U.S. NAVAL SUPPORT ACTIVITY
PSC 817 BOX 1
FPO AE 09622-0001

NAVSUPPACTNAPLESINST 5531.1
N19
11 OCT 2018

NAVSUPPACT NAPLES INSTRUCTION 5531.1

From: Commanding Officer, U.S. Naval Support Activity, Naples, Italy

Subj: INDUSTRIAL SECURITY PROGRAM

Ref: (a) E.O. 12829, National Industrial Security Program, January 6, 1993
(b) SECNAV M-5510.30
(c) DODI 5220.22, National Industrial Security Program (NISP), March 18, 2011
(d) DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), February 28, 2006
(e) DOD 5220.22-R, Industrial Security Regulation
(f) DoDM 5220.22, Vol 3, National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI), April 17, 2014
(g) SECNAV M-5510.36
(h) DoDM 5200.01, Vol 1–4, Information Security Program
(i) CNICINST 5531.1
(j) FAR Subpart 1.6, Career Development, Contracting Authority, and Responsibilities
(k) FAR Subpart 4.4, Safeguarding Classified Information Within Industry
(l) NAVSUP, NAVFAC and CNIC Memorandum of Understanding of July 20, 2004
(m) Defense Security Service 254 Guide, "A Guide for the Preparation of a DD Form 254, DoD Contract Security Classification Specification" of April 2011

Encl: (1) Contractors with Foreign Ownership, Control or Influence
(2) Sample Security Section of the Performance Work Statement

1. Purpose. This instruction prescribes policy and assigns responsibilities for industrial security for Commanding Officer (CO), U.S. Naval Support Activity (NAVSUPPACT), Naples, Italy and establishes, implements, and supplements process and procedures outlined in references (a) through (k) for industrial security. Additionally, this instruction provides guidance on contractors with Foreign Ownership, Control, or Influence (FOCI) if applicable, and advises as to the National Interest Determination (NID) approving authority, if applicable.

2. Scope and Applicability. This instruction applies to all agencies under NAVSUPPACT Naples that engage in classified procurement, or when cleared contractors operate within the areas under the CO's control. Currently, NAVSUPPACT Naples does not engage in classified procurement, however, cleared contractors operate under CO's control on the installation.

3. Policy

a. Per references (a) through (h), the National Industrial Security Program (NISP) was established for the protection of information classified under Executive Order 13526, as amended, and the Atomic Energy Act of 1954, as amended, placed within the hands or entrusted to the Defense

Industrial Base. The National Security Council is responsible for providing overall policy direction for the NISP. The Secretary of Defense has been designated lead agent for the NISP by the President of the United States. The Director, Information Security Oversight Office, is responsible for implementing and monitoring the NISP and for issuing implementing directives that are binding on agencies. Defense Security Service (DSS) is responsible for administering the Department of Defense (DoD) NISP on behalf of all DoD agencies, the Departments of the Navy, Army, and Air Force, to include their activities, and those federal agencies which have established NISP servicing agreements with DoD.

b. Per reference (l), Naval Supply Systems Command (NAVSUP) and Naval Facilities Engineering Command (NAVFAC) will provide the necessary contracting support to Commander, Navy Installations Command (CNIC) Region Activities. NAVSUP provides contracting authority to the Fleet and Industrial Supply Centers (FISC) and Navy Region Contracting Centers Naples and Singapore to perform their contracting mission. NAVFAC provides contracting authority to NAVFAC field activities to perform their contracting mission. This provides contracting support within their geographic Region to CNIC. NAVSUP and NAVFAC are responsible for identifying the alignment of its field contracting organizations to CNIC Regions.

4. Responsibilities

a. COs are responsible for:

(1) Establishing an industrial security program when the command engages in classified procurement, or when cleared contractors operate within areas under the CO's control.

(2) Appointing, in writing, a Command Security Manager (CSM) to implement industrial security for their installation, and ensuring the CSM has the tools, resources, and training necessary to successfully oversee information security for their activities.

(3) Appointing, in writing, an Industrial Security Program Manager (ISPM), who is appropriately qualified to manage an industrial security program at installation level; this duty may be assigned to the CSM or delegated to an Industrial Security Specialist under the CSM.

(4) Nominating Contracting Officer's Representatives (COR) in writing, and ensuring CORs are appointed per references (a) through (h) if applicable.

(5) Appointing a NID approving authority in writing, if applicable, for contracts with FOCI; see enclosure (1) for details, if applicable.

b. Contracting Officers are responsible for ensuring all industrial security duties are executed per references (b), (d), (e), and (i) through (k). NAVSUP and NAVFAC will provide the necessary contracting support for installation activities. Per reference (l), NAVSUP and NAVFAC will allocate contracting support based on the CNIC Installation Management Accounting Project, Installation Core Business Model.

c. ISPMs assigned to the contract are responsible for:

(1) Completing basic industrial security training requirements, via courses from the Center for Development of Security Excellence (CDSE); and COR training requirements via the Defense Acquisition University (DAU), if nominated as a COR.

(2) Ensuring all CORs have completed official COR training, and have been designated and authorized, in writing, by the Contracting Officer. The COR is responsible to the CSM for coordinating with Program Managers (PM) and technical and procurement officials.

(3) Ensuring one or more qualified security specialists have been designated, in writing, as CORs for classified contracts for the purpose of preparing and signing the DoD Contract Security Classification Specification (DD Form 254), and revisions thereto, and other security related contract correspondence.

(4) Reviewing all unclassified contracts, classified contracts with DD Forms 254, a Statement of Work (SOW), Statement of Objective (SOO), or Performance of Work Statement (PWS) received from the CSM, Contracting Officer, COR or PM prior to approval.

(5) Ensuring all active classified contracts include a valid DD Form 254, on file with DSS.

(6) Providing technical advice on proper completion and suggested CO changes, if any, on all DD Forms 254. Instructions for completing DD Form 254 may be found in reference (m).

(7) Ensuring unclassified contracts and DD Form 254's for classified contracts are updated and renewed, if applicable, in a timely manner.

(8) Ensuring DD Form 254's are not utilized on any unclassified contracts across installation activities.

(9) Coordinating with DSS on the completion of the DD Form 254 and other industrial security matters.

(10) Ensuring Operations Security (OPSEC), counterintelligence and supply chain risk management are considered and included in the framework of the contract preparation, in order to properly address the handling and protection of unclassified, classified, sensitive, intelligence and operations information, which may be required.

(11) Providing industrial security training annually or as necessary to all CORs, throughout their respective installation.

(12) Reporting adverse information to DSS that could affect the facility clearance level of a prime contractor.

d. CSM are responsible for:

(1) Completing basic industrial security training requirements, via courses from the CDSE; and COR training via the DAU, if nominated as a COR where applicable.

(2) Ensuring contractor personnel are aware of and adhere to local security policies and procedures.

(3) Receiving copies of contracts from CNIC, reviewing, and providing advice and assistance on all contracts, DD Form 254's, SOWs, SOOs, or PWSs prior to submission to the ISPM.

(4) Ensuring the correct level of access, position sensitivity and IT designation levels are verified and authorized on all contracts, DD Form 254's, SOWs, SOOs, or PWSs.

(5) Providing assistance, as needed, to the Contracting Officer, COR, PM or others, as assigned during the completion of the DD Form 254, and oversight of the security elements contained in the DD Form 254 and unclassified contracts as applicable.

(6) Providing assistance and information, as necessary, regarding industrial security issues or concerns to the CNIC and or Region ISPM, if applicable.

(7) Appointing, in writing, an industrial security specialist, or assistant to manage the industrial security program, if program is not managed by the CSM. However, the CSM will maintain overall responsibility for the Command Information Security Program.

e. CORs who are assigned to contract are responsible for:

(1) Completing basic industrial Security training requirements, via courses from the CDSE, and COR training via the DAU.

(2) Ensuring that the industrial security functions, specified in chapter 11 of reference (j), are accomplished when classified information is provided to industry for performance on a classified contract.

(3) Reviewing all proposed solicitations to determine whether access to classified information may be required by facility security officers or by contractors during contract performance.

(4) Ensuring contractor personnel have the appropriate security clearance and information technology access level, as stipulated in the SOW, SOO, or PWS.

(5) Informing contractors and subcontractors of the security classification and requirements assigned to the various documents, material, tasks, subcontracts and components of the classified contracts.

(6) Completing the DD Form 254 with a SOW, SOO, or PWS for the review of the ISPM.

(7) Coordinating with the appropriate CSM on any questions, concerns or issues regarding the completion of the DD Form 254.

(8) Ensuring a signed copy of the DD Form 254 is provided to all offices checked for distribution.

(9) Ensuring Visit Access Requests are approved and submitted to local activity security office via Joint Personnel Adjudication System.

(10) Ensuring contractor employees are properly brief on security procedures and requirements applicable to their duties.

(11) Monitoring personnel status changes of contractors, notifying the local Security Manager of contractor employee departures, and ensuring all government issued credentials (CAC, SIPR tokens) are retrieved prior to departure.

f. OPSEC Program Managers/Coordinators are responsible for conducting formal contract reviews to ensure that classified contracts properly reflect OPSEC requirements and responsibilities, when applicable.

5. Forms Management Control. DD Form 254, Contract Security Classification Specification and instructions to complete can be found at http://www.dss.mil/isp/tools.html.

6. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per SECNAV M-5210.1.

7. Review and Effective Date. Per OPNAVINST 5215.17A, NAVSUPPACT Naples will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after effective date unless reissued or canceled prior to the 5-year anniversary date, or an extension has been granted.

T. A. ABRAHAMSON

Releasability and distribution:
NAVSUPPACTNAPLESINST 5216.4BB
Lists: I through IV
Electronic via NAVSUPPACT Naples website:
https://www.cnic.navy.mil/regions/cnreurafswa/installations/nsa_naples/about/departments/administration_n1/administrative_services/instructions.html

Contractors with Foreign Ownership, Control or Influence

1. General

a. If a contractor performing on a classified contract has Foreign Ownership, Control or Influence (FOCI) or if the contract can be negated, the Defense Security Service (DSS) will inform the Commander, as such influence might jeopardize the security of classified information held by the contractor. DSS will advise the Activity of the requirement for a National Interest Determination (NID). The NID can be program, project or contract specific. A separate NID is not required for each contract under a program or project.

b. If an Activity considers sponsoring a NID, the requesting activity is to obtain written release approval authority from the functional owner of the prescribed information prior to submitting the NID to the contracting office. The justification from the requesting activity must address and explain how the FOCI contractor's product or service is crucial or is the sole available source. If applicable, they must also provide a written explanation when contract cancellation would cause unacceptable delays in the field or for support organizations. The Foreign Disclosure Officer and the TOP SECRET Control Officer for TOP SECRET, National Security Agency for Communications Security, the Office of Director National Intelligence (DNI) for sensitive compartmented information (SCI), and Department of Energy for restricted data or formerly restricted data, must be contacted to obtain release approval. (All NID involving SCI must be submitted to the Special Security Office for review before it is submitted to DNI.)

c. The NID and associated written approvals are reviewed, validated and processed by the Activity and the package is forwarded to DSS for the final approval.

d. Reference (f) contains procedures for government activities relating to FOCI.

2. NID Approving Authority. The NID decision is made by an authorized official of the Activity to certify, in writing, that there is a compelling need to issue the Limited Facility Clearance (FCL) and accept the risk inherent in not mitigating the FOCI. The FCL permits performance only on classified contracts issued by the activity that sponsored the company for the FCL. Each Region or activity should appoint a NID Approving Authority in writing, if applicable.

Sample Security Section of the Performance Work Statement

1. Security Requirements. State whether the work will be UNCLASSIFIED, CONFIDENTIAL, SECRET or TOP SECRET (TS), based on your knowledge of the requirement.

a. Submission. Include a Contract Security Classification Specification, DD Form 254, for all classified contracts. Use the fillable DD254.pdf version and submit with the requirements package. Processing a DD Form 254 for unique security requirements may extend the timeline to award the Contract.

b. Reminder. The SOW/PWS itself must be UNCLASSIFIED. If the contract-level DD Form 254 is not adequate for the project, this paragraph must include the required security level (as stated above) plus the statement, "Also see attached DD Form 254." The Contracting Officer's Representative (COR) must provide a task order-level DD Form 254 to include any security restraints or release constraints that will have an effect on performance of the tasks defined in the SOW.)

(1) Mandatory Security References (listed in Block 13): Command Security Manager (CSM) or cognizant Security Office will complete this section.

(2) Additional Security References (listed in Block 14): CSM or cognizant Security Office will complete this section.

2. Facility Security Clearance. The work to be performed under this contract is up to the TS level. Therefore the company must have a final Top Secret Facility Clearance (FCL) from the Defense Security Service (DSS) Facility Clearance Branch (FCB).

3. Security Clearance and Information Technology (IT) Level. All personnel performing on this contract will be U.S. citizens. There are three levels of personnel security requirements under this contract covering six types of positions: (These are examples only)

a. The following type of positions require a minimum of final TS security clearance and final IT-I (privileged level systems access) eligibility when performance starts:

(1) Senior System Administrator – NMCI

(2) Senior System Analysts – NMCI (two positions)

(3) System Administrator – NMCI (five positions)

b. If COR does not have TS, provide a POC with TS to monitor the work (example: all TS work will be monitored by John Doe).

c. The following type of positions require a minimum of Final Secret security clearance and IT-I eligibility when performance starts:

(1) Program Manager

(2) Project Manager

(3) Financial Analyst

d. The following positions require a minimum Interim Secret security clearance and interim IT-II eligibility when performance starts:

(1) Research Analyst

(2) Executive Assistant

6. Investigation Requirements. For TS and/or SCI Eligibility/Access or IT-I designation level: All personnel requiring SCI, TS or IT-I eligibility under this contract must undergo a favorably adjudicated Single Scope Background Investigation (SSBI)/Tier 5 (T5) as a minimum investigation. The SSBI/T5 will be current within five-years and requests for Special Background Periodic Review (SBPR)/Tier 5 Reinvestigation (T5R) will be initiated prior to the five-year anniversary date of the previous SSBI/T5 or SBPR/T5R.

7. Secret Eligibility/Access: All personnel requiring Secret under this contract must undergo a favorably adjudicated National Agency Check, Local Agency Check and Credit Check (NACLC)/Tier 3 (T3) as a minimum investigation. The NACLC/T3 will be maintained current within 10-years and requests for Secret Periodic Reviews (SPRs)/Tier 3 Reinvestigations(T3R) will be initiated prior to the 10-year anniversary date of the previous NACLC/T3 or SPR/T3R.

8. Contract employees that are not immediately eligible for at least interim IT-I systems access will be permitted to begin work with interim IT-II systems access at the discretion of the Government, pending eligibility for IT-I. Before being permitted to begin work under this arrangement the individual contractor employee must be submitted by the company for an SSBI (investigation) that is reflected in the DoD Joint Personnel Adjudication System (JPAS) database and granted interim IT-II systems access approval by the Activity Personnel Security. The employee will not be granted any privileged access until interim or final IT-I systems access is granted by the Security Management office. The contractor must submit the request for SSBI as soon as a job offer is tendered to an employee. Advance NAC results will be requested by the contractor to facilitate expeditious consideration for interim IT-I systems access by the Activity Security Office.

9. Advance NAC results or a previous DoD investigation are required for interim IT-I consideration. If the employee is not able to obtain an interim IT-I clearance within 90 days they will not be eligible to provide service on the contract.

10. For Access to Unclassified and Sensitive Government Information (not requiring a clearance): All personnel requiring access to Controlled Unclassified Information (e.g. For Official Use Only, Law Enforcement Sensitive, Personally identifiable information, etc.) under this contract must

undergo a favorably adjudicated suitability background investigation to determine fitness, per Executive Order 13467 and The Office of Personnel Management (OPM) Federal Investigative Standards.

11. The following meet the background investigation standard for access to unclassified government information:

a. High Risk positions have the potential for exceptionally serious impact on the integrity and efficiency of contractor support service. These positions involve duties that are especially critical to the agency or the program mission with a broad scope of responsibility and authority. The minimum investigative standard for a High Risk Public Trust Position is the T4 investigation; Reinvestigation is every five years.

b. Moderate Risk positions have the potential for moderate to serious impact on the integrity and efficiency of contractor support service. These positions involve duties that are considerably important to the agency or program mission with significant program responsibility or delivery of service. The minimum investigative standard for a Moderate Risk Public Trust Position is the T2 investigation; Reinvestigation is every five years.

c. Low Risk positions have the potential for limited impact on the integrity and efficiency of contractor support service. These positions involve duties and responsibilities of limited relation to the agency or program mission. The minimum investigative standard for a Low Risk position is the T1 investigation; Formerly the National Agency Check with Inquiries (NACI); Reinvestigation is every five years.

12. Adjudication for IT access. Adjudication of investigations for granting of interim or final IT-I access will be accomplished through the Activity Security Office. An exception to this is that individual contractor employees with an SSBI or SBPR (within a five-year scope) that is favorably adjudicated for a Top Secret security clearance by any of the Department of Defense Adjudication Facility (DoD CAF) will be automatically accepted for final IT-I access.

13. Interim IT access. Pending completion of a SSBI (for IT-I) and final adjudication for security clearance, contractor employees may be granted interim authorization to perform duties designated as IT-I. The interim authority for IT sensitive positions is the Activity.

14. Personnel Security Office. Following are the requirements, which must be met prior to granting of interim IT-I authorization:

a. The request for SSBI (E-QIP and fingerprint cards) must be submitted by the contractor Facility Security Officer (FSO) through the DSS to the Office of Personnel Management (OPM) and the Department of Defense (DoD) Personnel Security Data Base. JPAS must reflect that the investigation is open. A copy of the E-QIP forms must be submitted to the Activity Security Office, Security Manager (SM). The SM will forward the forms along with a written request for interim IT-I authorization to the Security Management office for approval.

b. NAC portion of the SSBI/T5 or a previous valid NCLC/DNACI/NAC or ENTNAC must be completed and favorably adjudicated before interim IT-I access will be granted. An interim security clearance (either TS or Secret, as appropriate for the position) should be requested by the company FSO for those contractor employees without a previous investigation.

15. Visit Authorization Requests (VAR). The Contractor will forward a VAR to the COR/Program Manager/SM via JPAS.

16. Information Security and Other Miscellaneous Requirements

a. Contractor personnel must comply with local security requirements for entry and exit control for personnel and property at the government facility. Contractor employees will be required to comply with all Government security regulations and requirements. Initial and periodic security training and briefings will be provided by Government security personnel. Failure to comply with security requirements is cause for removal and the contractor will not be able to provide service on this contract.

b. The Contractor will not divulge any information about DoD files, data processing activities or functions, user identifications, passwords, or any other knowledge that may be gained, to anyone who is not authorized to have access to such information. The Contractor will observe and comply with the security provisions in effect at the DoD facility. Identification will be worn and displayed as required.

c. Commanding Officer retains the right to request removal of contractor personnel regardless of prior clearance or adjudication status, whose actions, while assigned to this contract, clearly conflict with the interest of the Government.

d. Contractor personnel will generate or handle documents that contain For Official Use Only (FOUO) information at Government facilities. Contractors will have access to, generate, and handle classified material only at Government facilities. All contractor deliverables will be marked at a minimum FOUO, unless otherwise directed by the Government. The contractor will comply with the provisions of the DOD Industrial Security Manual for handling classified material and producing deliverables. The contractor will comply with the NAVSUPPACT Naples Industrial Security Instruction.