OPNAV INSTRUCTION 3900.30

From: Chief of Naval Operations

Subj: NAVY CAPABILITY PROTECTION CELL

Ref: (a) OPNAVINST 5450.352A
(b) SECNAVINST 3850.2E
(c) 50 U.S.C §4565
(d) DoD Instruction 2000.25 of 5 August 2010

1. **Purpose.** Per references (a) through (d), this instruction establishes policy and issues responsibilities for the Navy Capability Protection Cell (NCPC) to assess those areas where adversaries are most aggressively targeting the Navy’s warfighting advantage and to coordinate strategic courses of action (COA) to safeguard Navy equities.

2. **Background.** The Navy is faced with increasingly complex challenges to protect equities such as critical technologies and infrastructure, supply chains, and sensitive missions, training, and testing on Navy bases and ranges, from incursion, influence, and malign-intent. Global competitors, such as China, Russia, North Korea, Iran, and others, are strategically using the global economic commons to negatively impact U.S. military advantage; threaten American resiliency, critical infrastructure, and technological advantage; and encroach upon U.S. military testing and training areas and the Navy must account for this reality. NCPC is established to ensure continuity of awareness of these concerns, and recommend mitigation strategies across staffs of the Secretary of the Navy (SECNAV); Office of the Chief of Naval Operations (OPNAV); Commander, United States Fleet Forces Command; and Commander, Pacific Fleet.

3. **Scope**

   a. This instruction provides the organizational construct to facilitate the sharing of information among NCPC members who have identified threats through traditional analyses and to address modern challenges falling outside the scope of a traditional OPNAV code for action. The intent is to identify any strategies used by countries of concern to exploit vulnerabilities in existing foreign investment vetting processes and regulations. Examples of non-traditional emerging challenges include: foreign investment transactions involving sophisticated peer and near-peer state competitors; malign non-state actors; countries of concern access to advanced or disruptive technologies; and proximity to Navy training, testing, and operating areas within the United States and overseas.
This instruction facilitates the development of actions required to protect critical technology and infrastructure, to include task critical assets (TCA) and critical suppliers both within and outside of the traditional defense industrial base. These actions will align with the Office of the Secretary of Defense and Joint Staff efforts to pursue any strategy that prevents the degradation of the Navy’s warfighting and technological advantage to near-peer competitors. Leveraging existing Department of Defense (DoD) authorities and capabilities will enable NCPC to identify vulnerabilities in foreign industrial bases that can be exploited, degraded, manipulated, or otherwise negatively impact the Navy.

4. Policy. With support from echelon 2 commands, Secretary of the Navy, and other stakeholders, NCPC and echelon 1 members will:

a. facilitate and promote proactive protection of controlled technical information, especially where the information is particularly vulnerable to traditional and nontraditional foreign intelligence collection methods; and ensure communication between acquisition, intelligence, counterintelligence (CI), security, and law enforcement activities to assist in protection efforts;

b. early in the development cycle, identify and inform protection of technologies that present a high likelihood of disclosing unique and critical performance characteristics of military systems or manufacturing processes;

c. identify and prioritize critical acquisition programs, technologies, and infrastructure requiring proactive measures to enhance information and capability protection in order to apply scarce resources to the highest priorities;

d. coordinate and facilitate policy development, authority identification, implementation, sustainment guidance, governance, and resource planning for the proactive protection of controlled technical information; and

e. in collaboration with U.S. Government agencies and departments whose mission and authorities align, assist in monitor and assessing strategies to degrade the technological advantage of adversary countries.

5. Roles and Responsibilities. Chief of Naval Operations (CNO) assigns the NCPC primary responsibility to evaluate and inform actions to safeguard Navy equities. NCPC’s responsibilities are detailed in subparagraphs 5a through 5q.

a. Review, coordinate, and recommend:

(1) actions taken by existing Navy organizations with proper authorities; and

(2) controlled technical information protection efforts to proactively mitigate future losses.
b. Focus on maintaining warfighting advantage while informing and collaborating with the Joint Force to develop effective countermeasures and mitigations to the aforementioned emerging challenges described in paragraph 3.

c. Integrate all-source information by existing organizations with proper authorities in order to improve enterprise protection of controlled technical information. Provide scalable options for analyzing the increasing threat to technologies that reside in or transit the defense industrial base.

d. Leverage the Navy damage assessment management office to develop an enterprise view of impacts of compromises and other sources of controlled technical information loss.

e. Coordinate and facilitate policy development, authority identification, implementation, sustainment guidance, governance, and resource planning for the proactive protection of controlled technical information.

f. Lead efforts to leverage acquisition, intelligence, CI, security, mission assurance, risk management, threat and law enforcement data to inform methods, tools, authorities, and training requirements.

g. Coordinate and recommend methods, tools, processes, and procedures for Navy acquisition protection and exploitation countermeasures.

h. Seek, develop, or integrate new technologies and methodologies to mitigate controlled technical information and critical infrastructure threats and vulnerabilities.

i. Leverage Deputy Chief of Naval Operations for Fleet Readiness and Logistics (CNO N4) CNO-mission assurance assessment and risk management results to identify TCA, threats, and vulnerabilities.

j. Assimilate data and expertise regarding loss or potential loss of controlled technical information to inform requirements, acquisition, programmatic and strategic COAs.

k. Identify gaps in protection capabilities and recommend policy changes or other initiatives to improve controlled technical information protection.

l. Integrate critical acquisition and technology programs that require higher levels of information protection and propose appropriate methods of tiered protection measures.

m. Assess critical program information of research, development, technology, and evaluation programs identified in DoD Instruction 5200.39, Critical Program Information (CPI)
Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E) of 28 May 2015, as well as critical intelligence parameters and controlled technical information identified by security classification guides.

n. Oversee and contribute to the development and maintenance of the NCPC list of controlled technical information and critical infrastructure to guide controlled technical information identification and protection efforts.

o. Contribute in the development and maintenance of the Director, Shore Readiness Division (OPNAV N46) TCA list.

p. Coordinate, as needed, with the joint acquisition protection and exploitation cell, other Military Departments, and other Title 10 acquisition authority DoD component acquisition executives, to determine and address national security gaps and threats caused by foreign direct investment and economic statecraft.

q. Coordinate review of potential threats to critical technology and infrastructure through assessments of countries of concern for investments that could potentially impair the ability of the Department of the Navy (DON) to defend the Nation.

6. **NCPC Membership.** CNO N4, under the authority, direction, and control of reference (a), will serve as the office of primary responsibility for coordination of all Navy internal NCPC activities. Additionally, NCPC will meet, at a minimum, once per month to maintain situational awareness on emergent foreign investment or other identified activity that could negatively impact the Navy’s ability to maintain its warfighting advantage and national security.

   a. **Navy Echelon 1 Membership and Roles**

      (1) **Chair.** Director, Energy and Environmental Readiness Division (OPNAV N45) will serve as the Navy office of primary responsibility and NCPC representative for the review, investigation, and adjudication for Committee on Foreign Investment in the United States (CFIUS). The OPNAV N45 Foreign Direct Investment Branch (OPNAV N455) serves as the subject matter expert (SME) on all impacts to Navy readiness as a result of foreign investment in proximity to Navy installations, training, and testing ranges to include land, sea, airspace, and operating areas. OPNAV N455 will also serve as the SME for the review of foreign investment transactions and development and assessment of the effectiveness of possible mitigation compliance policies and methods applied to national security mitigation agreements negotiated with businesses to mitigate risks to national security involved in the foreign acquisition of United States businesses or land. OPNAV Installations Operations Branch (OPNAV N462) will serve as the SME for the identification and management of risk to TCA that support the execution of Navy missions, essential functions, and capabilities Navy wide.
(2) **Co-Chair.** Deputy Director, Innovation, Technology, Requirements and Test and Evaluation Division (OPNAV N94B), in conjunction with OPNAV N45, will review, investigate, and adjudicate CFIUS and intra-agency reviews and investigations. OPNAV N94B will evaluate threats to naval equities, critical technologies, supply chains, and critical infrastructure, and direct participation from the appropriate organization based on the equity involved.

(3) **Judge Advocate General of the Navy (OPNAV N09J).** A judge advocate from OPNAV N09J with a top secret and sensitive compartmentalized information security clearance will provide legal counsel with respect to matters before the NCPC, to include providing advice related to authorities for actions contemplated by the NCPC.

(4) **Deputy Chief of Naval Operations for Information Warfare (CNO N2N6)**

   (a) CNO N2N6 will serve as the primary member for delivery of threat intentions, threat technological developments, and current capabilities. Per reference (a), CNO N2N6 will leverage U.S. Navy CI authorities and capabilities to detect, deter, and deny these threats, in coordination with Naval Criminal Investigative Services (NCIS)/OPNAV N09N. CNO N2N6 will also serve as the liaison between NCPC and the intelligence community.

   (b) Director, Office of Commercial Economic Analysis (OCEA) (N2N6I22) is a multi-Service office focused on analyzing global macroeconomic trends relative to near-peer competitors. OCEA, in concert with private sector partners, conducts in-depth financial studies of technologies, manufacturing capabilities, and critical infrastructure concerns nominated by the NCPC. These studies are intended to illuminate previously unforeseen risks to the DoD’s warfighting advantage. OCEA then develops COAs which are presented to relevant key stakeholders for selection and implementation.

(5) **Deputy Chief of Naval Operations for Operations, Plans and Policy (CNO N3N5).**

   Director, Navy Eurasia Strategic Initiatives Division (OPNAV N53), will execute the CNO's Naval Strategy Panel and provide the CNO and Navy leadership with independent analysis on geo-strategic and political-military issues. In this capacity, OPNAV N53 will coordinate NCPC with the Naval Strategy Panel, to include biweekly working-level meetings and core group sessions, when required.

(6) **Deputy Chief of Naval Operations for Integration of Capabilities and Resources (CNO N8).** Director, Assessment Division (OPNAV N81), will provide assessments of NCPC topics as related to the impact on Navy programs.
(7) Deputy Chief of Naval Operations for Warfare Systems (CNO N9). Director, Innovation, Technology Requirements and Testing and Experimentation Division (OPNAV N94), will provide SME advice, input, and recommendations on foreign investment transactions related to technologies and proximity to the Navy training and testing ranges. OPNAV N94 will be the CNO N9 lead for NCPC coordination.

b. Navy Echelon 2 Membership. The participation of echelon 2 members is essential to the overall effectiveness of this effort. The intended role of echelon 2 commands referenced in subparagraphs 6b(1) through 6b(3) is to identify an NCPC point of contact to coordinate requests for information, such as subject matter expert support, to assist in the adjudication of foreign investment activities that pose a national security risk to the Navy.

(1) Commander, Pacific Fleet

(2) Commander, United States Fleet Forces Command

(3) Commander, Navy Installations Command

c. Department of the Navy Secretariat Participants

(1) Assistant Secretary of the Navy for Energy, Installations and Environment may participate on an ad hoc basis to support naval installation related CFIUS cases, control systems, cybersecurity, and critical infrastructure.

(2) Deputy Under Secretary of the Navy for Policy (DUSN (P)) may provide Secretariat-level advocacy and guidance on policies regarding all NCPC efforts. In addition, DUSN (P) may provide the requisite coordination across the DON to ensure all stakeholder equities are addressed.

(3) Deputy Assistant Secretary of the Navy for Research, Development, Testing and Experimentation may participate as required.

(4) Navy International Program Office may participate on an ad hoc basis to support acquisition related CFIUS cases.

d. Other Stakeholders

(1) United States Marine Corps (USMC). USMC may provide SME support to the NCPC to resolve mutual related concerns between Navy and USMC that are raised.

(2) NCIS/OPNAV N09N. NCIS/OPNAV N09N conducts an array of CI activities to help counter the threat posed by foreign intelligence entities. This includes full-spectrum CI operations, investigations, functional services, cyber, technical countermeasures, research,
analysis, and collections. NCIS/OPNAV N09N also partners with domestic and foreign law enforcement and security agencies to maximize the effective deployment of CI resources. Since 2011, NCIS/OPNAV N09N has used a threat-based analytic framework to prioritize technology protection known as the strategically prioritized acquisition matrix. This framework has helped influence similar efforts among other DoD organizations, most notably joint acquisition protection and exploitation cell and Defense Security Services. NCIS/OPNAV N09N also conducts joint CI operations and investigations with U.S. law enforcement agencies and U.S. intelligence community elements.

7. **Records Management.** Records created as a result of this instruction, regardless of media and format, must be managed per SECNAV Manual 5210.1 of January 2012.

8. **Review and Effective Date.** Per OPNAVINST 5215.17A, CNO N4 will review this instruction annually on the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 5 years, unless revised or cancelled in the interim, and will be reissued by the 5-year anniversary date if it is 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.

STEFFANIE B. EASTER  
Director, Navy Staff

Releasability and distribution:  
This instruction is cleared for public release and is available electronically only via Department of the Navy Issuances Web site, [http://doni.documentsservices.dla.mil](http://doni.documentsservices.dla.mil)