Department of Defense
INSTRUCTION

NUMBER 5200.39
May 28, 2015
Incorporating Change 1, November 17, 2017

USD(I)/USD(AT&L)

SUBJECT: Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues DoD Instruction (DoDI) 5200.39 (Reference (a)) in accordance with the authorities in DoD Directive (DoDD) 5143.01 (Reference (b)) and DoDD 5134.01 (Reference (c)).

b. Establishes policy and assigns responsibilities for the identification and protection of CPI.

c. Establishes policy in accordance with DoDD 5000.01 (Reference (d)) and DoDI 5000.02 (Reference (e)).

d. Incorporates and cancels the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) memorandum (Reference (f)).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of 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 within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. It is DoD policy that:

a. U.S. warfighter technological advantage will be maintained and operational effectiveness of DoD capabilities will be preserved through the identification and protection of CPI.

b. CPI will be identified early and reassessed throughout the RDT&E program so that CPI protections requirements and countermeasures may be identified and applied as the CPI is developed and modified throughout the lifecycle as needed.

c. CPI will be horizontally identified and protected to ensure equivalent protections are consistently and efficiently applied across programs based on the exposure of the system, consequence of CPI compromise, and assessed threats. Protections will, at a minimum, include anti-tamper, exportability features, security (cybersecurity, industrial security, information security, operations security, personnel security, and physical security), or equivalent countermeasures.

d. CPI protection measures will be integrated and synchronized, then documented within the Program Protection Plan (PPP) in accordance with Reference (e).

e. The original classification authority with program and supervisory responsibility for the CPI will conduct a review to make a determination of classification for vulnerabilities, to include by compilation, contained in the PPP, and issue security classification guidance in accordance with Volume 1 of DoD Manual (DoDM) 5200.01 (Reference (g)) and DoDM 5200.45 (Reference (h)).

4. RESPONSIBILITIES. See Enclosure 2.

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

6. EFFECTIVE DATE. This instruction is effective May 28, 2015.

Marcel Lettre
Acting Under Secretary of Defense
for Intelligence

Frank Kendall
Under Secretary of Defense
for Acquisition, Technology, and Logistics

Enclosures
1. References
2. Responsibilities

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008, as amended (hereby cancelled)
(b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," October 24, 2014, as amended
(c) DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005, as amended
(d) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003, as amended
(e) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015*, as amended*
(f) Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Horizontal Protection of DoD Critical Program Information," July 22, 2010 (hereby cancelled)
(g) DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012
(h) DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," April 2, 2013
(i) DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, as amended
(j) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999
(k) DoD Directive 5530.3, "International Agreements," June 11, 1987, as amended
(l) DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014
(m) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
(n) DoD Directive 5105.42, "Defense Security Service (DSS)," August 3, 2010, as amended
(o) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014
(p) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010
(q) DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," February 6, 2013
(r) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(s) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014*, as amended*
(t) Intelligence Community Directive Number 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 15, 2008
(u) DoD 5220.22-R, "Industrial Security Regulation," December 4, 1985, as amended
(v) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
(w) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended

(x) Committee on National Security Systems Instruction Number 4009, "National Information Assurance (IA) Glossary," April 26, 2010, as amended

~~(y) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition~~

(y) Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

(z) DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012*, as amended*

(aa) DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012*, as amended*

(ab) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). In addition to the responsibilities in section 8 of this enclosure, the USD(I):

a. Establishes policy and provides oversight for counterintelligence (CI), intelligence, and security support to CPI identification and protection in accordance with Reference (b).

b. Serves as the DoD focal point and OSD Principal Staff Assistant to the Secretary and Deputy Secretary of Defense on all CPI matters in coordination with the USD(AT&L) and in coordination with the Under Secretary of Defense for Policy (USD(P)) on matters pertaining to CPI protection in international programs.

c. Requires, in coordination with the USD(AT&L) and the USD(P), that appropriate training, as identified in DoDI O-5240.24 (Reference (i)), is available for CI, intelligence, security, and RDT&E personnel regarding the identification and protection of CPI, to include the role each must perform.

d. Oversees and directs the Defense Intelligence Components in the production of threat assessments to help mitigate the risk of CPI compromise.

2. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 7 of this enclosure, the Director, DIA:

a. Supports the Defense Intelligence Components in validating foreign intelligence threat.

b. Produces intelligence and counterintelligence assessments, to include the technology targeting risk assessments (TTRAs), to help DoD Components identify threats to CPI.

3. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). Under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 7 of this enclosure, the Director, DSS:

a. Coordinates the execution of a DoD Component counterintelligence support plan (CISP) at cleared defense contractor facilities with CPI in accordance with Reference (i).

b. Develops and provides training for DoD and defense contractor security personnel regarding CPI protection activities required by (or in) classified contracts.

c. Provides unclassified and classified all-source analyses, to include, but not limited to, annual analyses of suspicious contacts and activities occurring within the defense contractor community that could adversely affect the protection of CPI. Disseminates reports to the defense contractor community and DoD Component heads.

4. USD(AT&L). In addition to the responsibilities in section 8 of this enclosure, the USD(AT&L):

a. Establishes policy and guidance, in coordination with the USD(I) and the DoD Component heads, for the identification, protection, and reassessment of CPI.

b. Develops training for RDT&E personnel required to identify and protect CPI, in coordination with the USD(I) and DoD Component heads.

c. Controls, oversees, and manages the Acquisition Security Database (ASDB) for the horizontal identification and protection of CPI in coordination with the DoD Component heads.

d. Establishes policy and oversees anti-tamper (AT) policies, procedures, and processes for the protection of CPI in accordance with Reference (e).

e. Oversees the consideration, planning, and design of defense exportability features into systems with CPI in accordance with Reference (e).

f. Oversees the identification and protection of CPI in special access programs (SAPs) to include horizontal protection.

5. USD(P). In addition to the responsibilities in section 8 of this enclosure, the USD(P):

a. Provides policy oversight for international technology transfer activities, including export controls, to support the protection of CPI, in accordance with DoDD 5111.1 (Reference (j)), DoDD 5530.3 (Reference (k)), and DoDI 2040.02 (Reference (l)).

b. Establishes and oversees the implementation of policy for international security countermeasures, including provisions for protecting CPI during negotiations of agreements with foreign governments and international organizations, to support the protection of CPI in accordance with References (j), (k), and (l) and DoDD 5230.11 (Reference (m)).

c. Develops training for the DoD Components and defense contractors on the protection of CPI as it relates to security and export control arrangements for international programs, pursuant to DoDD 5105.42 (Reference (n)).

6. CHIEF INFORMATION OFFICER OF THE DEPARMENT OF DEFENSE (DoD CIO). In addition to the responsibilities in section 8 of this enclosure, the DoD CIO provides policy,

guidance, and oversight for the protection of DoD information technology processing CPI in accordance with DoDD 5144.02 (Reference (o)).

7. DoD COMPONENT HEADS. The DoD Component heads:

a. Identify and protect inherited and organic CPI for RDT&E programs in accordance with policy and guidance established in paragraphs 1a and 4a of this enclosure.

b. Assess identified CPI for appropriate classification in accordance with the original classification process described in Reference (g).

c. Assign DoD Component CI, intelligence, security, operations security, foreign disclosure, system engineering, system security engineering, AT, cybersecurity, and other specialists to support the identification and protection of CPI.

d. Train DoD Component RDT&E personnel to properly identify and protect CPI in accordance with this enclosure.

e. Ensure horizontal identification and protection, utilizing the ASDB when conducting horizontal identification and protection analysis. Input and validate program information, including inherited and organic CPI, into the ASDB.

f. Identify and protect CPI in SAPs in accordance with DoDD 5205.07 (Reference (p)) and DoDI 5205.11 (Reference (q)). References (p) and (q) have precedence over this instruction until the SAP is transitioned to collateral or unclassified status.

g. Provide CI support to RDT&E programs with CPI in accordance with Reference (i).

h. Prepare CISPs for all DoD Component-designated RDT&E facilities and defense contractor facilities with CPI in accordance with Reference (i).

i. Secure DoD information technology storing, processing, or transmitting CPI in accordance with DoDI 8500.01 (Reference (r)) and DoDI 8510.01 (Reference (s)). Sensitive compartmented information systems will be certified and accredited in accordance with Intelligence Community Directive 503 (Reference (t)). SAP information systems will comply with the requirements in References (p) and (q).

j. Report incidents of loss, compromise, or theft of CPI in accordance with procedures in Reference (i), DoD 5220.22-R (Reference (u)), and Volume 3 of DoDM 5200.01 (Reference (v)), as appropriate.

8. OSD COMPONENT HEADS WITH APPROVAL AUTHORITY OR MILESTONE DECISION AUTHORITY (MDA) FOR RDT&E PROGRAMS. The OSD Component heads with approval authority or MDA for RDT&E programs oversee the horizontal identification and

protection of inherited and organic CPI for their respective RDT&E programs in accordance with policy and guidance established in paragraphs 1a and 4a of this enclosure.

9. SECRETARY OF THE AIR FORCE (SAF). In addition to the responsibilities in section 7 of this enclosure, the SAF:

a. Establishes AT guidance in coordination with the USD(AT&L).

b. Assesses, in coordination with the affected DoD Component head, the effectiveness and the implementation of the AT plan, an appendix to the PPP, and advises the responsible MDA or equivalent, in writing, of the adequacy of the plan at the appropriate milestone.

c. Establishes and conducts AT training and outreach programs.

d. Conducts DoD-wide analysis of AT protections in support of horizontal protection.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASDB	Acquisition Security Database
AT	anti-tamper
CI	counterintelligence
CISP	counterintelligence support plan
CPI	critical program information
DIA	Defense Intelligence Agency
DoD CIO	Chief Information Officer of the Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
DSS	Defense Security Service
MDA	milestone decision authority
PPP	program protection plan
RDT&E	research, development, test, and evaluation
SAF	Secretary of the Air Force
SAP	special access program
TTRA	technology targeting risk assessment
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this instruction.

ASDB. The DoD horizontal protection database providing online storage, retrieval, and tracking of CPI and supporting program protection documents to facilitate comparative analysis of defense systems' technology and align CPI protection activities across the DoD.

AT. Systems engineering activities intended to prevent or delay exploitation of CPI in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering.

CISP. Defined in Reference (i).

compromise. Defined in Reference (g).

consequence of CPI compromise. The impact, if the CPI is compromised, on U.S. tactical or strategic military advantage, and the time and resources required for the U.S. to re-gain that tactical or strategic military advantage.

contractor. Defined in DoDM 5220.22 (Reference (w)).

contractor facilities. Locations where access to classified information occurs in the performance of legitimate requirements for such access.

countermeasures. The employment of devices or techniques that impair the operational effectiveness of enemy activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities.

CPI. U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.

Defense Intelligence Components. Defined in Reference (b).

exposure. The likelihood that an adversary will be able to obtain the end-item; operational environment is a primary factor.

focal point. In a particular organization (e.g., the headquarters of a major command), the principal point of contact for coordination and exchange of information related to a particular issue or area.

horizontal identification. Consistent determination of CPI across two or more RDT&E programs as a result of a formal CPI identification process.

horizontal protection. Application of a consistent level of protection to similar CPI associated with more than one RDT&E program, including inherited CPI.

information technology. Defined in the Committee on National Security Systems Instruction Number 4009 (Reference (x)).

inherited CPI. CPI that is owned and generated by one RDT&E program, subsystem, or project that is incorporated into and used by another RDT&E program.

lifecycle. Defined in ~~Joint Publication 1-02~~ *the DoD Dictionary of Military and Associated Terms* (Reference (y)).

organic CPI. Unique CPI that is owned and generated by an RDT&E program.

PPP. A risk-based, comprehensive, living plan to guide efforts for managing the risks to CPI and mission-critical functions and components.

RDT&E. Defined in DoDI 5230.24 (Reference (z)).

system security engineering. Defined in DoDI 5200.44 (Reference (aa)).

threat. An assessment of foreign adversary interest and skill in obtaining CPI.

TTRA. A country-by-country assessment conducted by the DoD entities within the Intelligence Community, as defined in Executive Order 12333 (Reference (ab)), that quantifies risks to CPI and related enabling technologies for weapons systems; advanced technologies or programs; facilities such as laboratories, factories, research and development sites (e.g., test ranges); and military installations. The TTRA evaluates five independent risk factors, each of which contributes to an overall risk factor. The five areas evaluated are: technology competence, national level of interest, risk of technology diversion, ability to assimilate, and technology protection risk.