



Department of Defense INSTRUCTION

NUMBER 5200.39

July 16, 2008

USD(I)

SUBJECT: Critical Program Information (CPI) Protection Within the Department of Defense

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive 5200.39 (Reference (a)) as a DoD Instruction in accordance with the guidance in DoD Instruction 5025.01 (Reference (b)) and the authority in DoD Directive 5143.01 (Reference (c)).

(1) Establishes policy for the protection of CPI.

(2) Issues policy and assigns responsibility for counterintelligence (CI), Intelligence, Security, and Systems Engineering support for the identification and protection of CPI.

(3) Assigns responsibilities to DoD Components relating to the identification of CPI and the implementation of plans for its protection.

b. Provides policy on and implements relevant parts of DoD Directive 5000.01 (Reference (d)) and DoD Instruction 5000.2 (Reference (e)).

c. Authorizes the issuance of additional guidance, consistent with Reference (b).

d. Continues to authorize the publication of DoD 5200.1-M (Reference (f)) as the overarching implementing issuance for this Instruction until such time that it is replaced. Where inconsistencies exist between this Instruction and Reference (f), this Instruction shall supersede.

e. Supplements existing policies and guidance related to the security of DoD personnel, information, resources, installations, and operations to include DoD contractors performing work or supporting a DoD research, development, and acquisition (RDA) effort (e.g., DoD Directive 5205.02 (Reference (g)), DoD 5200.1-R (Reference (h)), or DoD 5200.08-R (Reference (i))).

2. APPLICABILITY. This Instruction applies to:

a. 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 Department of Defense (hereafter referred to collectively as the “DoD Components”).

b. DoD contractors performing work on or supporting DoD contracts with contractual terms that require the contractor to protect CPI.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy:

a. To provide uncompromised and secure military systems to the warfighter by performing comprehensive protection of CPI through the integrated and synchronized application of CI, Intelligence, Security, systems engineering, and other defensive countermeasures to mitigate risk. Failure to apply consistent protection of CPI may result in the loss of confidentiality, integrity, or availability of CPI, resulting in the impairment of the warfighter’s capability and DoD’s technological superiority.

b. To mitigate the exploitation of CPI, extend the operational effectiveness of military systems through application of appropriate risk management strategies, employ the most effective protection measures, to include system assurance and anti-tamper (AT), and document the measures in a Program Protection Plan (PPP) (see Glossary and Reference (f)).

c. To conduct comparative analysis of defense systems’ technologies and align CPI protection activities horizontally throughout the Department of Defense.

d. To identify CPI early in the technology development, acquisition, and sustainment process; refine at each milestone or as directed by the Milestone Decision Authority (MDA); and to initiate and maintain the appropriate protection of CPI throughout its military life cycle.

e. To require all RDA programs with CPI to submit a PPP for review and approval by the appropriate MDA or science and technology (S&T) equivalent per Reference (e).

f. To assure federally funded products of fundamental research remain unrestricted to the maximum extent possible according to National Security Decision Directive 189 (Reference (j)).


g. To minimize the chance that the Department’s warfighting capability will be impaired due to the compromise of elements or components being integrated into DoD systems by foreign intelligence, foreign terrorist, or other hostile elements through the supply chain or system design.

h. To require that contracts supporting RDA programs where CPI has been identified shall contain contractual terms requiring the contractor to protect the CPI to the standards articulated in this Instruction.

5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. UNLIMITED. This Instruction is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at <http://www.dtic.mil/whs/directives>.

7. EFFECTIVE DATE. This Instruction is effective immediately.



James R. Clapper, Jr.
Under Secretary of Defense for Intelligence

Enclosures

1. References
 2. Responsibilities
- Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5200.39, "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection," September 10, 1997 (hereby canceled)
- (b) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
- (c) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),
November 23, 2005
- (d) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
- (e) DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003
- (f) DoD 5200.1-M, "Acquisition Systems Protection Program," March 1994
- (g) DoD Directive 5205.02, "DoD Operations Security (OPSEC) Program," March 6, 2006
- (h) DoD 5200.1-R, "Information Security Program," January 1997
- (i) DoD 5200.08-R, "Physical Security Program," April 9, 2007
- (j) National Security Decision Directive 189, "National Policy on the Transfer of Scientific, Technical, and Engineering Information," September 21, 1985¹
- (k) DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," January 17, 1984
- (l) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (m) DoD Directive 5530.3, "International Agreements," June 11, 1987
- (n) DoD 5105.38-M, "Security Assistance Management Manual," October 3, 2003
- (o) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
- (p) DoD Directive 5105.42, "Defense Security Service (DSS)," May 13, 1999
- (q) DoD Directive 5205.07, "Special Access Program (SAP) Policy," January 5, 2006
- (r) DoD Instruction O-5205.11, "Management, Administration, Oversight of DoD Special Access Programs (SAPs)," July 1, 1997
- (s) DoD Instruction 5240.6, "Counterintelligence (CI) Awareness, Briefing, and Reporting Programs," August 7, 2004
- (t) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
- (u) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (v) DCI Directive 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," June 5, 1999²
- (w) DoD Directive 0-5240.02, "Counterintelligence," December 20, 2007
- (x) DoD Instruction 5240.18, "Counterintelligence Analysis and Production," December 4, 2006
- (y) DoD Directive 5105.67, "Department of Defense Counterintelligence Field Activity (DoD CIFA)," February 19, 2002

¹ Document is available at: <http://www.aau.edu/research/itar-nsdd189.html>

² Available through the Controlled Access Program Coordination Office, http://capco.dssc.sgov./dcids_home.htm

- (z) Part 126 of title 22, Code of Federal Regulations
- (aa) National Intelligence Estimate, “Cyber Threats to the U.S. Information Infrastructure”³
- (ab) DoD 4140.1-R, “DoD Supply Chain Materiel Management Regulation,” May 23, 2003

³ Document is classified. Available through the National Intelligence Council,
http://www.dni.gov/nic/NIC_home.html

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), in accordance with Reference (c), shall:

- a. Provide policy and oversight for CI, Intelligence, and Security support to CPI protection.
- b. Serve as the advisor and OSD Principal Staff Assistant to the Secretary and Deputy Secretary of Defense on all matters pertaining to CI, Intelligence, and Security support to CPI protection.
- c. Serve as the DoD focal point on all policy matters involving CPI that require coordination with non-DoD Federal law enforcement, security, or intelligence agencies.
- d. Collaborate with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)); the Under Secretary of Defense for Policy (USD(P)); and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) to require that appropriate training is available to CI, Intelligence, Security, and RDA personnel regarding the identification and protection of CPI, to include the role each must perform.
- e. Require the establishment of a database, and designate a responsible organization, in coordination with the USD(AT&L) and the ASD(NII)/DoD CIO, for utilization by RDA organizations to record and track CPI for horizontal protection, compromise, and analysis purposes. Special Access Programs (SAPs) and Sensitive Compartmented Information (SCI) are exempt from mandatory inclusion in this database.
- f. Issue policy guidance that requires the Heads of DoD Components with CI elements and organizations to develop and implement tailored CI Support Plans (CISPs) at all DoD research and development facilities, RDA programs with CPI, and at cleared Defense contractors with CPI.
- g. Issue policy guidance that requires the Heads of DoD Components with intelligence and CI analytical centers to provide assessments regarding foreign intelligence requirements for and targeting of CPI.
- h. Issue policy guidance that requires the Heads of DoD Components with security organizations to assist RDA program managers in the development and implementation of PPPs for the protection of CPI, from identification until such protection is no longer required, in accordance with Reference (f).

i. Provide advice and guidance to USD(AT&L) to establish procedures outlining the PPP development and approval process, in coordination with the ASD(NII)/DoD CIO, USD(P), and DoD components for all RDA programs with CPI.

j. Provide advice and guidance to USD(AT&L) and the ASD(NII)/DoD CIO to establish a consistent process for the identification of CPI that takes into account the role RDA, CI, Intelligence, Security, and systems engineering personnel perform.

k. Collaborate with the USD(AT&L) and the ASD(NII)/DoD CIO to establish procedures in coordination with the DoD Component Special Access Program Central Offices (SAPCOs) to identify CPI early in the technology development and acquisition process and initiate protection of CPI from the point of identification until such protection is no longer required.

l. Establish an all-source threat assessment capability to protect CPI against Supply Chain Vulnerabilities within the Department of Defense.

m. Collaborate with the USD(AT&L) and the ASD(NII)/DoD CIO to develop guidance to mitigate risks identified in Supply Chain Vulnerabilities in RDA programs assessed to contain CPI.

2. USD(AT&L). The USD(AT&L) shall:

a. Lead the effort, in collaboration with the USD(I) and the ASD(NII)/DoD CIO, to establish a consistent process for the identification and protection of CPI that takes into account the role RDA, CI, Intelligence, Security, and systems engineering personnel perform.

b. Provide direction and management oversight for the identification and protection of CPI for RDA programs under USD(AT&L) cognizance or oversight.

c. Require a PPP for all RDA programs with CPI within the purview of the USD(AT&L) and establish procedures outlining the PPP development and approval process in coordination with the USD(I), ASD(NII)/DoD CIO, USD(P), and the DoD Components.

d. Lead the collaboration with the ASD(NII)/DoD CIO and the DoD Components for review of Major Defense Acquisition Program (MDAP) PPPs for sufficiency prior to its Defense Acquisition Board (DAB) milestone decision reviews and at major Acquisition Strategy updates.

e. Collaborate with the USD(I) and the ASD(NII)/DoD CIO to require that appropriate training is available to RDA personnel regarding the identification and protection of CPI; to include the roles RDA, sustainment (logistics, maintenance, repair, supply), testing, CI, Intelligence, Security, systems engineering, and information systems security engineering (ISSE) personnel perform.

f. Collaborate with the USD(I) and the ASD(NII)/DoD CIO to establish procedures in coordination with the DoD Component SAPCOs to identify CPI early in the technology

development and acquisition process and initiate protection of CPI from the point of identification until such protection is no longer required.

g. Provide, in collaboration with the ASD(NII)/DoD CIO and the AT Executive Agent (ATEA), oversight of AT implementation and policy development that is in concert with this Instruction and Reference (e), and applicable to CPI protection efforts in accordance with Reference (f).

h. Provide guidance and oversight to mitigate Supply Chain Vulnerabilities in RDA programs assessed to contain CPI within the purview of the USD(AT&L). Guidance should be developed in coordination with the USD(I) and the ASD(NII)/DoD CIO.

i. Establish guidance to implement the provisions of the PPP for DoD contractors.

j. Provide systems engineering guidance and oversight for the mitigation of CPI vulnerabilities within the Global Information Grid.

k. Establish procedures in coordination with the USD(I) and the ASD(NII)/DoD CIO for identifying and entering CPI and Defense technologies into the horizontal protection database, for horizontal protection purposes, for RDA programs under the USD(AT&L) cognizance or oversight.

3. USD(P). The USD(P) shall:

a. Establish policy and exercise oversight regarding the export and disclosure of CPI to foreign governments and international organizations in support of international RDA according to this Instruction, DoD Directive 2040.2 (Reference (k)), and DoD Directive 5230.11 (Reference (l)).

b. Establish policy and exercise oversight for the protection of CPI during negotiations of agreements with other governments or international organizations, concurrent with References (k) and (l), DoD Directive 5530.3 (Reference (m)), and DoD 5105.38-M (Reference (n)).

c. Establish policy and exercise oversight for the preparation of the Technology Assessment/Control Plan (TA/CP), the Delegation of Disclosure Authority Letter (DDL), and the Program Security Instruction.

d. Establish policy, exercise oversight, and develop related training for the DoD Components and DoD contractors on security and export control arrangements for international RDA programs pursuant to Reference (l), DoD Directive 5230.20 (Reference(o)), and DoD Directive 5105.42 (Reference (p)).

4. ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO shall:

- a. Provide oversight for Major Automated Information System (MAIS) programs with CPI to ensure compliance with this Instruction and References (e) and (f).
- b. Identify minimum security requirements for contractor owned and operated information systems for the protection of CPI.
- c. Provide ISSE guidance to ensure technical mitigation of supply chain vulnerabilities within systems, networks, and outsourced Information Technology (IT)-based services within the Global Information Grid.
- d. Lead the collaboration with the USD(AT&L) and the DoD Components for reviews of MAIS programs and MAIS-MDAP PPPs for sufficiency, as delegated by USD(AT&L), to ensure compliance with this Instruction and References (e) and (f) prior to its Information Technology Acquisition Board (ITAB) milestone decision review.
- e. Collaborate with the USD(I) and the USD(AT&L) to establish a consistent process for the identification of CPI that takes into account the role RDA, CI, Intelligence, Security, and systems engineering personnel perform.
- f. Collaborate with the USD(I) and the USD(AT&L) to require that appropriate training is available to RDA personnel regarding the identification and protection of CPI; to include the role RDA, CI, Intelligence, Security, systems engineering, and ISSE personnel perform.
- g. Provide direction and management oversight for the identification and protection of CPI for RDA programs under ASD(NII)/DoD CIO cognizance or oversight.
- h. Collaborate with the USD(I) and USD(AT&L) to establish procedures in coordination with the DoD Component SAPCOs to identify CPI early in the technology development and acquisition process and initiate protection of CPI from the point of identification until such protection is no longer required.
- i. Require a PPP for all RDA programs with CPI within the purview of the ASD(NII)/DoD CIO and provide advice and guidance to USD(AT&L) to establish procedures outlining the PPP development and approval process in coordination with the USD(I), USD(P), and the DoD Components.
- j. Establish procedures in coordination with the USD(I) and the USD(AT&L) to ensure CPI and defense technologies are entered into the horizontal protection database, for horizontal protection purposes, for RDA programs under ASD(NII)/DoD CIO cognizance or oversight.
- k. Provide guidance and oversight to mitigate Supply Chain Vulnerabilities in RDA programs assessed to contain CPI within the purview of the ASD(NII)/DoD CIO. Guidance should be developed in coordination with the USD(I) and the USD(AT&L).

l. Provide, in collaboration with the USD(AT&L) and the ATEA, oversight of AT implementation and policy development that is in concert with this Instruction and Reference (e), and applicable to CPI protection efforts in accordance with Reference (g).

m. Participate in the horizontal analysis of DoD technologies in support of the horizontal protection of CPI.

5. INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE (IG DoD). The IG DoD shall:

a. Provide oversight of component IG audits, evaluations, inspections, and law enforcement activities for compliance with this Instruction and related issuances.

b. Develop a uniform system of periodic inspections, using the existing DoD Component inspection process, for RDA organizations' compliance with applicable issuances concerning CPI.

c. Develop and maintain inspection guidelines for DoD-wide IGs to enhance the consistent application of this Instruction and related issuances as applied to the protection of CPI.

d. Publish a fiscal year inspection schedule listing RDA organizations subject to either Department of Defense or DoD Component IG inspections.

e. Publish an annual report of significant findings, recommendations, and best practices.

6. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Establish policies, plans, and procedures for the implementation of this Instruction.

b. Plan for and program the resources necessary to implement the requirements of this Instruction, to include the requirements for U.S. programs abroad.

c. Assign DoD Component CI, Intelligence, Security, Operations Security (OPSEC), Foreign Disclosure, systems engineering, ISSE, and AT specialists to support the RDA communities' identification and protection of CPI.

d. Assess RDA projects and programs for CPI in coordination with servicing CI, Intelligence, Security, ISSE, and systems engineering elements.

e. Develop and implement for review a PPP for all DoD Component RDA programs and projects with CPI.

f. Identify DoD Component MDAs or S&T equivalent to approve the PPP with the assistance of the component CI, intelligence, and security element. PPP approval and/or

recommendations for MDAP and MAIS Programs shall be provided to the USD(AT&L) and the ASD(NII)/DoD CIO in support of the DAB, the ITAB, and the Defense Space Acquisition Board.

g. Direct the utilization of the horizontal protection database by DoD Component RDA, Security, Intelligence, CI, OPSEC, Foreign Disclosure, systems engineering, and AT personnel, in order to execute their respective mission support requirements for the protection of DoD Component CPI.

h. Coordinate with the DoD Component SAPCO to identify CPI early in the technology development and acquisition process and initiate protection of CPI from the point of identification until such protection is no longer required. The unique nature of SAPs requires compliance with special security procedures and specific program guidance. DoD Directive 5205.7 (Reference (q)) and DoD Instruction O-5205.11 (Reference (r)) take precedence over this Instruction until a decision is made to transition the SAP to collateral or unclassified status.

i. Provide training on safeguarding CPI to all DoD Component and contractor personnel with access to CPI that is commensurate with their functional responsibilities or consistent with contractual requirements.

j. Establish procedures using the IG DoD guidelines for periodic inspections of RDA programs, within the continental United States (not related to classified contracts) and outside the continental United States, to evaluate compliance with requirements to protect CPI established by this Instruction.

k. Direct DoD Component intelligence analytical centers, in cooperation with the Defense Intelligence Agency (DIA), to provide Technology Targeting Risk Assessments (TTRA) to assist RDA programs with mitigating the risk of CPI compromise and to support CI organizations with developing CI Assessments of CPI.

l. Direct DoD Component CI analytical centers to provide CI Assessments for RDA programs with CPI.

m. Direct that all personnel with access to CPI disclose in advance instances of foreign travel to the DoD Component CI or Security organizations according to DoD Instruction 5240.6 (Reference (s)).

n. Exercise final approval authority for designating CPI unless the application of the technology is already designated as CPI elsewhere in the Department of Defense.

o. Direct all DoD information systems and networks storing, processing, or transmitting CPI comply with the requirements of DoD Directive 8500.01E (Reference (t)), implement the appropriate baseline Information Assurance (IA) controls from DoD Instruction 8500.2 (Reference (u)), and are accredited in accordance with the DoD IA Certification and Accreditation Process. For SAP and SCI, DCI Directive 6/3 (Reference (v)) procedures will be followed.

p. Direct that contractual agreements are in place that implement and validate appropriate IA requirements as identified by the DoD CIO, for all contractor and sub-contractor information systems and networks storing, processing, or transmitting CPI.

q. Require the integration of CI, Intelligence, Security, and systems engineering in a process to identify CPI and develop a PPP for its protection.

r. Report incidents of loss, compromise, or theft of CPI and AT breaches in accordance with procedures in Reference (h) and DoD Directive O-5240.02 (Reference (w)), as appropriate.

s. Direct the DoD Component CI analytical centers to provide appropriate CI Awareness Products to supported research and development centers and RDA programs to increase awareness of potential threats to CPI in accordance with DoD Instruction 5240.18 (Reference (x)), as appropriate.

t. Direct Component CI organizations to prepare CISPs at all Component research and development facilities, when CPI is identified in Component RDA programs, and at cleared Defense contractor facilities with CPI.

u. Coordinate with DoD and Service Acquisition Authorities to develop Service Department specific guidance to mitigate Supply Chain Vulnerabilities in RDA programs assessed to contain CPI.

7. DIRECTOR, DIA. The Director, DIA, under the authority, direction, and control of the USD(I), shall:

a. Lead and coordinate the DoD Component Intelligence Centers' production of TTRAs to assist RDA programs with mitigating the risk of CPI compromise and support CI organizations in developing CI Assessments of CPI.

b. Provide support to DoD Component CI Elements on horizontal protection analysis issues involving CPI.

c. Support the DoD Component CI organizations in validating foreign Intelligence and CI threat information to assist the MDA or S&T equivalent during program reviews of PPPs.

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

a. Assist the DoD Component CI elements in coordinating the execution of a CISP at cleared Defense contractors with CPI.

b. During the conduct of regularly scheduled security inspections at cleared Defense contractor facilities, determine if there are any contractually imposed protection measures for CPI related to classified contracts at these locations.

c. Develop and conduct training for DoD and Defense contractor security personnel regarding CPI protection activities.

d. Disseminate suspicious activity or equivalent reports, including those related to CPI, to the cognizant DoD Component CI element.

e. Implement the relevant provisions contained in Reference (s) within the cleared Defense contractor community.

f. Publish an unclassified and classified product detailing suspicious contacts occurring within the cleared Defense contractor community and provide appropriate dissemination of these reports to the DoD CI community, National entities, and the cleared Defense contractor community.

9. DIRECTOR, DoD COUNTERINTELLIGENCE FIELD ACTIVITY. The Director, DoD Counterintelligence Field Activity, under the authority, direction, and control of the USD(I), shall:

a. Coordinate with DIA and DoD Component CI elements on horizontal protection and analysis issues involving the protection of CPI.

b. Provide program management for DoD CI's support to the protection of CPI in accordance with DoD Directive 5105.67 (Reference (y)).

c. Develop and conduct training for DoD CI personnel regarding CPI protection activities.

d. Coordinate with the Director, DSS, and DoD Component CI elements regarding contractor protection of CPI.

10. DoD ATEA. The DoD ATEA, under the authority, direction, and control of the USD(AT&L), shall:

a. Develop AT policy to include procedures for notification of an AT breach incident involving CPI and AT applications for horizontal protection.

b. Utilize and maintain both AT technology and implementation databases, in coordination with appropriate DoD Components, to facilitate AT horizontal protection analysis involving CPI.

c. Assess the effectiveness and the implementation of the AT plan, (an annex to the PPP per Reference (e)), and advise the responsible MDA or equivalents in writing of the adequacy of the plan at appropriate acquisition milestones.

d. Establish procedures for implementing proper AT mechanisms for the protection of CPI during RDA programs.

e. Include AT requirements, capabilities, and limitations to protect CPI in AT education and outreach programs for the RDA organizations.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
AT	anti-tamper
ATEA	Anti-Tamper Executive Agent
CI	counterintelligence
CISP	Counterintelligence Support Plan
CPI	Critical Program Information
DAB	Defense Acquisition Board
DCHC	Defense Counterintelligence and Human Intelligence Center
DDL	Delegation of Disclosure Authority Letter
DIA	Defense Intelligence Agency
DSS	Defense Security Service
IA	information assurance
IG DoD	Inspector General of the Department of Defense
ISSE	information systems security engineering
IT	information technology
ITAB	Information Technology Acquisition Board
MAIS	Major Automated Information System
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
OPSEC	operations security
PPP	Program Protection Plan
RDA	research, development, and acquisition
S&T	science and technology
SAP	Special Access Program

SAPCO	Special Access Program Central Office
SCI	sensitive compartmented information
TA/CP	Technology Assessment / Control Plan
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, the following terms and their definitions are for the purposes of this Instruction only.

acquisition program. Defined in Reference (d).

AT. Systems engineering activities intended to deter and/or delay exploitation of critical technologies in a U.S. defense system in order to impede countermeasure development, unintended technology transfer, or alteration of a system.

ATEA. The DoD ATEA, chartered by the USD(AT&L), and assigned to the Directorate for Special Programs, Office of the Assistant Secretary of the Air Force for Acquisition.

CI assessment. A DoD Component's comprehensive analysis or study of a relevant CI topic, event, situation, issue, or development. CI assessments require exhaustive amounts of research and the production timeline can range from days to months (Reference (v)). When conducted in support of an RDA program with CPI, the assessment describes the threat a foreign entity (person, representative, corporation, government, military, commercial, etc.) represents to the CPI/system assessed. The assessment is multidisciplinary as it includes an analysis of the diverse foreign collection modalities available, the relative effectiveness of each, and capability of the foreign entity to collect information about research efforts, the technology, and/or system under development. The assessment may include the impact to the Department of Defense if the technology is compromised and be complimentary to, integrated with, or independent of the TTRA provided by the Defense Intelligence Community.

CI awareness products. A DoD Component's analysis of a CI topic, event, situation, issue, or development. These products differ from an assessment in that they are often time sensitive, are published as needed or annually, and normally do not require extensive research to produce. Products of this nature ensure a consistent flow of appropriately classified or categorized threat information is available to the community to increase awareness and action as appropriate. The Defense Security Service "Technology Collection Trends in Defense Industry" and the Office of

the National Counterintelligence Executive “Annual Report to Congress on Foreign Economic Espionage” are examples of products meeting this objective. CI products meeting this objective include CI Analysis Reports, CI Analysis Summaries, and CI Analysis Special Products (Reference (v)).

CISP. A formal plan that outlines and describes the CI support to be provided to research and development facilities, RDA programs with CPI, and CPI resident at cleared Defense contractor facilities. CISPs are coordinated with and approved by the RDA Director, Program Executive Office, or Program Manager, as appropriate, and are an appendix to the PPP.

country of concern. Includes countries on any of the following lists:

Nation states named in the State Department’s list of State Sponsors of Terrorism (part 126 of title 22, Code of Federal Regulations (Reference (z)));

Nation states that are named in the International Traffic in Arms Regulations (Reference (z)) for which exports and sales are prohibited as a matter of policy;

Nation states against which the United States maintains an arms embargo (Reference (z));

Nation states named in National Intelligence Estimates, to include “Cyber Threats to the U.S. Information Infrastructure” (Reference (aa)).

CPI. Elements or components of an RDA program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.

Includes information about applications, capabilities, processes, and end-items.

Includes elements or components critical to a military system or network mission effectiveness.

Includes technology that would reduce the US technological advantage if it came under foreign control.

CPI information shall be identified early in the research, technology development and acquisition processes, but no later than when a DoD Agency or military component demonstrates an application for the technology in an operational setting, in support of a transition agreement with a pre-systems acquisition or acquisition program, or in exceptional cases, at the discretion of the laboratory/technical director.

Pre-systems acquisition and acquisition programs shall review their programs for CPI when technologies are transitioned from research and development or inherited from another program, during the technology development phase, throughout program progression, and as directed by the MDA.

DDL. Defined in Reference (f)

horizontal protection analysis. The process that determines if critical Defense technologies, to include CPI, associated with more than one RDA program are protected to the same degree by all involved DoD activities.

ISSE. An engineering process that captures and refines information protection requirements and ensures their integration into IT acquisition processes through purposeful security design or configuration.

PPP. A risk-based, comprehensive, living plan to protect CPI that is associated with an RDA program. The PPP is used to develop tailored protection guidance for dissemination and implementation throughout the program for which it is created. The layering and integration of the selected protection requirements documented in a PPP provide for the integration and synchronization of CPI protection activities throughout the Department of Defense. The following are considered key elements of a PPP and are tailored to meet the requirements of an RDA program:

Technology and Project Description or System and Program Description with an emphasis on what is unique as the foundation for identifying CPI.

List of CPI to be protected in the program (this generally describes classified CPI in an unclassified manner and is not suitable for horizontal protection analysis or the preparation of a CI Assessment).

Threats to CPI.

Foreign threat.

A summary of the CI assessment (the principal report is an attachment).

Vulnerabilities of CPI to identified threats.

Countermeasures.

Security countermeasures (all disciplines, as appropriate).

CISP

AT annex (Reference (e)).

OPSEC plan.

System assurance.

Other countermeasures (unspecified).

TA/CP (References (e) and (m)).

Classification guides.

Protection costs.

Follow-on Support.

Program Security Instruction. Is supplementary to the national security rules of the participants under which classified information and material are normally protected. It should be used to reconcile differences in national policies so that standard procedures will be used for the program/project and to consolidate in a single security document the other security arrangements for a project, program, or contract (e.g., hand carriage, transportation plan). When a program or project involves the use of both national and North Atlantic Treaty Organization procedures, special attention must be given to differences in the procedures, particularly with regard to access control.

RDA. Defined in Reference (e)

supply chain management. A cross-functional approach to procuring, producing, and delivering products and services to customers. The broad management scope includes sub-suppliers, suppliers, internal information, and funds flow according to DoD 4140.1-R (Reference (ab)).

supply chain vulnerabilities. An assessment of the supply chain related to CPI to determine if an adversary has the capability and intent to affect it in a manner that compromises the military effectiveness of the given platform, weapon system, or network.

supplier assurance. Evidence demonstrating the level of confidence that a supplier is free from vulnerabilities.

system assurance. The justified measures of confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle.

TA/CP. The document that identifies and describes sensitive program information; the risks involved in foreign access to the information; the participation in the program or foreign sales of the resulting system; and the development of access controls and measures necessary to protect the U.S. technological or operational advantage of the system.

TTRA. A country-by-country assessment conducted by the Defense Intelligence Community that quantifies risks to CPI and related enabling technologies for weapons systems, advanced technologies or programs, and facilities such as laboratories, factories, research and development sites (test ranges, etc.), 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. The TTRA and CI Assessment provide laboratory/technical directors and Program Managers with information required to establish a comprehensive security program for the protection of identified CPI.