Department of Defense

INSTRUCTION

NUMBER O-5240.24
June 8, 2011

USD(I)

SUBJECT: Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. In accordance with the authority of DoD Directive (DoDD) 5143.01 (Reference (a)) and DoDD O-5240.02 (Reference (b)), establishes policy, assigns responsibilities, and provides procedures for the conduct of the CI activities supporting RDA.

b. Implements policy established in DoD Instruction (DoDI) 2040.02 (Reference (c)), DoDI 5200.39 (Reference (d)), and Directive-Type Memorandum 09-016 (Reference (e)) for CI support.

c. Directs the integration of a technology targeting risk assessment (TTRA) with the appropriate CI analytical product to address foreign collection threats to RDA programs with critical program information (CPI).

d. Provides for threat analysis to support supply chain risk management (SCRM).

e. Establishes the CI RDA Integrated Management Group (CI RDA IMG).

2. APPLICABILITY. This Instruction applies to:

a. The 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 DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereafter referred to collectively as the "DoD Components").

b. Active and reserve military personnel, DoD civilians, and contractor personnel when applied by contract (hereafter referred to collectively as "DoD personnel").

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that CI activities within the Defense CI enterprise shall:

a. Support, synchronize, and be integrated into RDA programs including research and engineering (R&E) activities governed under DoDD 5143.3 (Reference (f)); the Defense Acquisition System governed under DoDD 5000.01 and DoDI 5000.02 (References (g) and (h)); and activities associated with international transfers or exports of defense-related technology governed under Reference (c), DoD 5105.38-M, and DoDI 2030.08 (References (i) and (j)).

b. Not interfere with, restrict, or hinder the conduct of contracted fundamental research in accordance with National Security Decision Directive 189 and Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) Memorandum on fundamental research (References (k) and (l)).

c. Detect, assess, exploit, penetrate, degrade, counter, or neutralize foreign collection activity that threatens:

(1) RDA programs with CPI.

(2) Activities at DoD-affiliated research, development, test, and evaluation (RDT&E) facilities to include University Affiliated Research Centers (UARC) and Federally Funded Research and Development Centers (FFRDC).

(3) DoD personnel participating in a defense personnel exchange program (DPEP), liaison officer program, other international exchange programs conducted pursuant to DoDD 5530.3 (Reference (m)), visits and assignments of foreign nationals to RDT&E facilities, RDA programs, and cleared defense contractors (CDC), conducted pursuant to DoDD 5230.20 (Reference (n)).

(4) To obtain CPI or defense-related technology via illegal exports or illegal diversion via technology transfers.

(5) Capabilities of a CDC.

(6) The RDA supply chain to include information and communication technology designated as a critical component in a covered system.

d. Use the CI Support Plan (CISP) to identify CI support activities required for RDA programs with CPI, for DoD Component-designated RDT&E facilities; and for CDCs where RDA program CPI is located.

e. Document, in a USD(I)-approved information technology archiving system, activities conducted or initiated to support RDA in accordance with Reference (b) and DoDD 5015.2 (Reference (o)).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. INFORMATION REQUIREMENTS. The information requirement in this Instruction is exempt from licensing in accordance with paragraphs C4.4.1., C4.4.7., and C4.4.8. of DoD 8910.1-M (Reference (p)).

8. RELEASABILITY. This Instruction is approved for restricted release. It is available to users with Common Access Card authorization on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

9. EFFECTIVE DATE. This Instruction is effective immediately upon its publication to the DoD Issuances Website.

Michael G. Vickers
Under Secretary of Defense
for Intelligence

Enclosures
1. References
2. Responsibilities
3. Procedures
4. Coordinating CI Support
5. CI RDA IMG Charter

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(b) DoD Directive O-5240.02, "Counterintelligence," December 20, 2007
(c) DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," July 10, 2008
(d) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008
(e) Directive-Type Memorandum 09-016, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems," March 25, 2010
(f) DoD Directive 5134.3, "Director of Defense Research and Engineering (DDR&E)," November 3, 2003
(g) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
(h) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008
(i) DoD 5105.38-M, "Security Assistance Management Manual (SAMM)," October 3, 2003
(j) DoD Instruction 2030.08, "Implementation of Trade Security Controls (TSC) for Transfers of DoD U.S. Munitions List (USML) and Commerce Control List (CCL) Personal Property to Parties Outside of DoD Control," May 23, 2006
(k) National Security Decision Directive 189, "National Policy on the Transfer of Scientific, Technical, and Engineering Information," September 21, 1985, as amended
(l) Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Fundamental Research," May 24, 2010
(m) DoD Directive 5530.3, "International Agreements," June 11, 1987
(n) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
(o) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
(p) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998
(q) DoD Directive 5105.21, "Defense Intelligence Agency (DIA)," March 18, 2008
(r) DoD Instruction O-5100.93, "Defense Counterintelligence (CI) and Human Intelligence (HUMINT) Center (DCHC)," August 13, 2010
(s) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004
(t) DoD Instruction S-5240.09, "Offensive Counterintelligence Operations (OFCO) (U)," October 29, 2008
(u) Title 10, United States Code
(v) DoD Instruction 5240.10, "Counterintelligence Support to the Combatant Commands and the Defense Agencies," May 14, 2004
(w) DoD Instruction 5240.16, "DoD Counterintelligence Functional Services," May 21, 2005
(x) DoD Instruction 5240.05, "Technical Surveillance Countermeasure (TSCM) Program," February 2, 2006
(y) DoD Instruction 5240.06, "Counterintelligence (CI) Awareness, Briefing, and Reporting

Programs," August 7, 2004
(z) DoD Instruction O-5240.21, "Counterintelligence (CI) Inquiries," May 14, 2009
(aa) DoD Instruction S-5140.23, "Counterintelligence (CI) Activities in Cyberspace (U)," December 13, 2010
(ab) DoD Instruction S-5240.17, "Counterintelligence Collection (U)," January 12, 2009
(ac) DoD Instruction 5240.04, "Counterintelligence (CI) Investigations," February 2, 2009
(ad) DoD Instruction C-5205.01, "DoD Foreign Military Intelligence Collection Activities (FORMICA) (U)," January 22, 2009
(ae) DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010
(af) DoD Instruction 2000.25, "DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States (CFIUS)," August 5, 2010
(ag) National Intelligence Priorities Framework, current edition[1]
(ah) The National Threat Identification and Prioritization Assessment, current edition[2]
(ai) DoD Instruction 5240.18, "Counterintelligence (CI) Analysis and Production," November 17, 2009
(aj) Director of Central Intelligence Directive (FOUO) 7/6, "Community Acquisition Risk Center," March 2, 2005[3]
(ak) National Security Presidential Directive-54/Homeland Security Presidential Directive-23, "Cyber Security and Monitoring," July 8, 2008[2]
(al) The National Counterintelligence Executive, "The United States Government-Wide Cyber Counterintelligence Plan," current edition[2]
(am) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982
(an) Director of Central Intelligence Directive (S) 6/6, "Security Controls of the Dissemination of Intelligence Information (U)," July 11, 2001 [3]
(ao) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008
(ap) DoD 5200.1-R, "Information Security Program," January 1997
(aq) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006
(ar) DoD Instruction 5240.19, "Counterintelligence Support to the Defense Critical Infrastructure Program," August 27, 2007
(as) DoD Instruction C-5240.08, "Counterintelligence Security Classification Guide (U)," December 7, 2005
(at) DoD 7000.14-R, "Department of Defense Financial Management Regulations (FMRs)," Volume 2B, Chapter 5, Section 050201, July 2008
(au) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition
(av) Section 3542 of title 44, United States Code
(aw) DoD Directive 8500.01E, "Information Assurance," October 24, 2002

[1] Available to authorized users at http://www.intelink.ic.gov/wiki/NIPF
[2] Available from the Counterintelligence Directorate, DUSD(HCI&S)/CI, Room 3C1088, 5000 Defense Pentagon, Washington, DC 20301-5000
[3] Available to authorized users at http://www.intelink.ic.gov/PPR/strategyPlansPolicy.intel

(ax) Sections120-130 of title 22, Code of Federal Regulations
(ay) Parts 730-774 as amended, of title 15, Code of Federal Regulations
(az) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984
(ba) Section 11101 of title 40, United States Code
(bb) Technology Readiness Assessment (TRA) Deskbook, current edition[4]

[4] Available to authorized users at http://www.dod.gov/ddre/doc/dod_tra_july_2009_read_version.pdf

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), shall:

a. Monitor implementation of this Instruction and issue additional direction and guidance as may be necessary.

b. Resolve any issue concerning CI activities supporting RDA that cannot be resolved by the DoD Components.

2. DEPUTY UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (DUSD(I&S)). The DUSD(I&S), under the authority, direction, and control of the USD(I), shall:

a. Develop policy and conduct policy oversight assessments of CI activities supporting RDA.

b. Represent OSD at DoD and national-level forums concerning CI activities supporting RDA.

3. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the USD(I), in addition to responsibilities in DoDD 5105.21 (Reference (q)) and sections 9 and 10 of this enclosure, shall:

a. Provide intelligence assessments and estimates in support of RDA and CI activities supporting RDA described in section 1 of Appendix 1 to Enclosure 3.

b. Establish collection requirements in support of RDA and SCRM.

4. DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE CENTER (DCHC). The Director, DCHC, under the authority, direction, and control of the Director, DIA, in addition to the responsibilities in accordance with DoDI O-5100.93 (Reference (r)), shall:

a. Provide functional management of CI activities supporting RDA to:

(1) Chair the CI RDA IMG.

(2) Maintain an information technology (IT) system and architecture for the Defense CI Components to record and conduct analysis of official and non-official visits and assignments of

foreign nationals to DoD RDA facilities or programs. In accordance with DoDI 4630.8 (Reference (s)), ensure the system is interoperable with appropriate national systems and USD(I)-approved IT systems.

(3) Exchange appropriate information with the Under Secretary of Defense for Policy (USD(P)) or the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))-managed IT systems (e.g., the Security and Policy Analysis Network (SPAN) and horizontal protection database) with DCHC-managed IT systems.

(4) Support the DoD technology security program by informing the USD(P) and the USD(AT&L) of illegal exports of defense-related technology based on reporting collected from the Military Department CI Organizations (MDCO).

(5) Develop and execute specialized training for personnel conducting CI activities supporting RDA in accordance with Reference (r), and consistent with Enclosure 3, section 5.

(6) Coordinate with the Defense CI Components to develop performance measures for CI activities supporting RDA.

(7) Participate in DoD and national-level forums concerning CI activities supporting RDA.

b. Oversee execution of CI activities supporting RDA to:

(1) (U//FOUO) Determine foreign intelligence entity (FIE) interest in and targeting of emerging, enabling, and disruptive defense-related technology associated with critical capabilities prescribed by the Secretary of Defense annual planning and programming guidance (see Enclosure 3, section 2.)

(2) Manage the threat analysis center supporting SCRM in accordance with section 4 of Appendix 1 to Enclosure 3.

(3) Coordinate and conduct offensive CI operations (OFCO) supporting RDA in accordance with DoDI S-5240.09 (Reference (t)) and manage activities with international partners in accordance with Reference (r).

(4) Appropriately integrate CI analysis with intelligence assessments and estimates supporting RDA as described in section 1 of Appendix 1 to Enclosure 3.

(5) Conduct assessments of CI activities supporting RDA in accordance with Reference (r).

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

a. Conduct authorized CI activities supporting RDA at CDCs in accordance with Enclosure 3, section 3, and provide analytical support consistent with section 2 of Appendix 1 to Enclosure 3.

b. Serve as the CI focal point for the USD(AT&L)-designated accreditation authority for trusted suppliers (the Defense Microelectronics Activity) of application-specific integrated circuits (ASICs).

c. Develop, in collaboration with the Federal Bureau of Investigation (FBI) and appropriate DoD and OSD Components, a process for the FBI to inform DoD of suspicious foreign collection activity reported by defense industry and CDCs to the FBI.

d. Provide DSS industrial security and CI-related information to the USD(AT&L)-managed horizontal protection database.

e. Train personnel to conduct authorized CI activities supporting RDA at CDCs.

6. USD(P). The USD(P), shall:

a. Exchange appropriate information between USD(P)-managed IT systems (e.g., SPAN) with DCHC-managed IT systems.

b. Inform the Director, DIA of defense articles and services selected for enhanced end use monitoring (EEUM) and request analytical support as appropriate.

7. ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO, shall inform the Director, DIA, of requirements for CI collection supporting SCRM.

8. USD(AT&L). The USD(AT&L), shall:

a. (U//FOUO) Inform the Director, DCHC, of emerging, enabling, and disruptive technology associated with critical capabilities prescribed by the Secretary of Defense annual planning and programming guidance (see Enclosure 3, section 2.)

b. Inform the Director, DSS, of a company or CDC accredited as an ASIC trusted supplier.

c. Exchange appropriate information between USD(AT&L)-managed IT systems (e.g., the horizontal protection database) and DCHC-managed IT systems.

d. Coordinate with the Director, Defense Logistics Agency (DLA), and the Director, DCHC, to determine threat analysis requirements to support DLA SCRM requirements and to support the trade security control (TSC) assessment process established in Reference (i).

9. HEADS OF DoD COMPONENTS WITH A DEFENSE CI COMPONENT. The Heads of the DoD Components that have a Defense CI Component, excluding the Director, DSS, shall:

a. Conduct authorized CI activities supporting RDA described in Enclosure 3, and associated appendixes.

b. Appoint a CI subject matter expert to provide advice and assistance to the Component Acquisition Executive.

c. Support USD(AT&L)-managed horizontal technology protection initiatives.

d. Support the DoD Component milestone decision authority (MDA) determine sufficiency of CI support during reviews of a Component RDA program protection plan (PPP).

e. Conduct CI activities with international partners in support of RDA programs and international transfers or exports defense-related technology in accordance with References (b), (r), and (t).

f. Coordinate, synchronize, and deconflict CI activities supporting RDA with the Component human intelligence (HUMINT) element as appropriate.

g. Coordinate the conduct of CI activities at a CDC with local DSS CI personnel and with the FBI for activities at an FFRDC or UARC.

h. Train personnel to conduct authorized CI activities supporting RDA.

10. HEADS OF THE DoD COMPONENTS AUTHORIZED TO ENGAGE IN RDA. The Heads of the DoD Components authorized to engage in RDA pursuant to title 10, United States Code (U.S.C.) (Reference (u)), in addition to responsibilities in Reference (d) and section 9 of this enclosure, shall:

a. Appoint an official to coordinate CI activities described in Enclosure 4.

b. Coordinate the conduct of CI activities at UARCs with the supporting Defense CI Component in accordance with Enclosure 3, section 3 that comport with References (k) and (l).

c. Coordinate the conduct of CI activities supporting international transfers and exports of defense-related technology with the supporting Defense CI Component in accordance with Enclosure 3, section 4.

d. Request threat analysis of supply chain risk from the Director, DCHC, to support Component SCRM requirements in accordance with section 4 of Appendix 1 to Enclosure 3.

11. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments, in addition to the responsibilities in sections 9 and 10, shall, in accordance with DoDI 5240.10 (Reference (v)), assist the OSD, designated Defense Agencies, DoD Field Activities, and the Commander, United States Special Operations Command (USSOCOM), to conduct authorized CI activities in accordance with Enclosure 3, section 3 that exceed their organic capabilities.

ENCLOSURE 3

PROCEDURES

1. MISSION. The CI mission in RDA informs the DoD Components and supporting CDCs of foreign collection threats and detects FIE targeting of defense-related technology. The CI support enables RDA program personnel to implement countermeasures and enables CI to develop activities that negate, counter, penetrate, or exploit an FIE.

2. (U//FOUO) ACTIVITIES SUPPORTING THE USD(AT&L). Upon notification from the USD(AT&L) that emerging, enabling, or disruptive technology associated with critical capabilities prescribed by the Secretary of Defense annual planning and programming guidance was selected, the Director, DCHC:

a. (U//FOUO) In collaboration with the science and technical intelligence elements of the IC, and DoD technology subject matter experts, conduct all-source analysis with the objective of determining foreign interest in and requirements for the defense-related technology associated with a capability (e.g., the critical foreign military need).

b. (U//FOUO) Provide analytical outcomes (e.g., assessments, reports, operational support packages) indicating critical foreign military needs and FIE targeting of this technology to the USD(AT&L) and, in conjunction with the USD(AT&L), determine requirements for CI activities up to and including OFCO and coordinate OFCO in accordance with Reference (t).

3. CI ACTIVITIES SUPPORTING RDA. CI activities supporting RDA:

a. Are based upon providing supported RDA programs with CI functional services in accordance with DoDI 5240.16, DoDI 5240.05, DoDI 5240.06, and DoDI O-5240.21 (References (w), (x), (y), and (z)). These activities may include:

(1) CI activities in cyberspace in accordance with DoDI S-5240.23 (Reference (aa)).

(2) CI collection in accordance with DoDI S-5420.17 (Reference (ab)).

(3) CI investigations in accordance with DoDI 5240.04 (Reference (ac)).

(4) (U//FOUO) OFCO in support of DoD Component RDA programs in accordance with Reference (t).

b. Specific CI activities include:

(1) Providing foreign collection threat information to assist RDA program personnel during the process to identify CPI and assisting in development of threat-based countermeasures implemented by a PPP.

(2) Conducting liaison with the FBI, the Defense Criminal Investigative Organizations, and other federal and state law enforcement agencies to exchange information regarding FIE activity and foreign collection threats to RDA.

(3) Participating in installation-level, program-level, or facility-level threat working groups to inform participants of foreign collections threats to RDA activities.

(4) Informing personnel at supported RDA programs, foreign military sales (FMS) programs, and facilities on the foreign technical surveillance collection threat in accordance with Reference (x).

(5) Coordinating with security managers, intelligence, and information assurance personnel to aid in threat identification and the establishment of countermeasures designed to detect and mitigate foreign and international terrorist cyber-associated threats to RDA programs and activities.

(6) Reviewing unsolicited requests for information to determine if defense-related technology is targeted by a FIE.

(7) Reviewing RDA-affiliated documents, program protection plans, and Intelligence Information Reports to assist in developing threat awareness training and requesting analytical support.

(8) Evaluating individual and organizational awareness of foreign collection threats to determine vulnerabilities to FIE collection, assessing the effectiveness of existing countermeasures, and assisting RDA security personnel develop new countermeasures.

(9) Providing foreign collection threat assessments, advisories, or related IC analytical products to supported RDT&E facilities, RDA programs with CPI, CDCs, and for use in constructing threat awareness training.

(10) Assisting program, company, or CDC security personnel to assess threats from visits, assignments, and employment of foreign nationals.

(11) Conducting threat awareness training for all supported RDA programs and conducting debriefings as necessary. In addition to the requirements of Reference (y), threat awareness training in RDA shall:

(a) Inform DoD personnel that information indicating defense-related technology was improperly diverted into a foreign military system is reportable in accordance with DoDI C-5205.01 (Reference (ad)).

(b) Focus on personnel who have: knowledge and access to CPI; process freedom of information act requests or requests for patent and copyright information; award contracts, grants or other contractual instruments; are involved in marketing, product sales, or exports of defense-related technology; participate in symposiums; or travel in official or non-official capacity to countries or locations where the risk from foreign intelligence-related activity is likely.

(c) Support the DoD foreign visit program, including, but not limited to DoD personnel who participate in a DPEP, serve as a liaison officer, are involved in a cooperative program or other international assignment program, or serve as a host for a foreign visitor or foreign assignee. DoD personnel assigned outside the United States for periods in excess of 30 days shall, as appropriate, be debriefed upon completion of the assignment.

c. CI activities supporting RDA are documented in the CISP as described in Appendix 2 of this enclosure.

4. ACTIVITIES IN EXPORT CONTROL AND TECHNOLOGY TRANSFER

a. The MDCOs collaborate with the FBI, the Department of Homeland Security, Immigration and Customs Enforcement, and Department of Commerce, Office of Export Enforcement, and the Defense Criminal Investigative Organizations, to assist these agencies supporting RDA equities in defense industry. The MDCOs:

(1) Provide these agencies with information to increase awareness within these agencies of defense-related technology critical to the national defense and locations within defense industry where such technologies are being developed, produced, or worked, and information pertaining to foreign collection activity threatening RDA activities.

(2) Assess information from these agencies pertaining to improperly exported defense-related technology and determine if an FIE is involved. Inform the Director, DCHC, of illegally exported technology to enable the USD(AT&L) and the USD(P) to assess the impact these activities have on the DoD technology security program and RDA programs.

(3) Assist in threat awareness training to enable defense industry to be aware of FIE activities that threaten technology critical to the national defense.

(4) Support the DLA-managed TSC process described in Reference (i).

(5) Support cyber intrusion damage assessments affecting RDA programs conducted pursuant to DoDI 5205.13 (Reference (ae)).

b. The Defense CI Components support their component activities for international programs, technology transfer, or exports. The Defense CI Components:

(1) Provide DIA produced risk assessments for technology transfer pertaining to a country's willingness and capability to protect defense-related technology and associated IC assessments describing the foreign intelligence threats posed in or from a specific country.

(2) Conduct threat awareness training for Defense Security Cooperation Agency (DSCA) and/or Defense CI Component personnel traveling to conduct an EEUM compliance assessment visit and conducting debriefings as necessary.

(3) Evaluate technology transfers and exports (e.g., FMS, EEUM) for opportunities to engage in a bilateral or multilateral relationship with international partners, and, when appropriate, jointly conducting CI activities to support the RDA program or activity.

(4) Support the Director, DSS, conduct analysis of current or potential CDCs to determine the nature and extent of foreign ownership control or influence issues.

(5) Support the Director, Defense Technology Security Administration, with assessments in support of the Committee on Foreign Investment in the United States in accordance with DoDI 2000.25 (Reference (af)). Assessments of this nature should address the potential threat the proposed transaction may pose for Component activities.

5. TRAINING. Training for personnel conducting CI activities supporting RDA shall include instruction on R&E, system engineering, the DoD acquisition process, CPI identification process, visits and assignments of foreign nationals, personnel exchange programs, export control, international transfers of technology, SCRM, and disposal or demilitarization of defense-related technology.

APPENDIX 1 TO ENCLOSURE 3

ANALYSIS

1. ANALYTICAL SUPPORT. The Director, DIA shall:

a. Produce an intelligence and CI assessment of the multidisciplinary foreign collection threats to RDA that conforms with the National Intelligence Priorities Framework, the National Threat Identification and Prioritization Assessment (References (ag) and (ah)), or as directed by the USD(I).

b. The assessment serves as a baseline to inform the RDA community of common foreign collection threats and to support program protection planning in accordance with References (d) and (h). The assessments shall be periodically updated and, to the extent possible, include information on:

(1) (U//FOUO) Foreign targeting of defense-related technology.

(2) (U//FOUO) Defense-related technology that would fulfill a critical foreign military need.

(3) (U//FOUO) A foreign entity's capability to conduct collection using computer network attack/exploitation, HUMINT, geospatial intelligence, measurement and signature intelligence, signals intelligence, open source intelligence, and collection using close-in or proximity technical means.

c. Produce a TTRA supporting CI analysis of foreign collection threats to RDA programs with CPI in accordance with Reference (d) and this appendix.

d Provide analytical support to the Director, DSCA, regarding transfers of defense related technology selected for EEUM in accordance with References (c) and (q).

2. CI ANALYTICAL PRODUCTS

a. CI analysis in RDA is conducted and products produced in accordance with DoDI 5240.18 (Reference (ai)), unless otherwise exempted by this Instruction or by the USD(I).

b. Defense CI Components conducting analysis in RDA shall provide products identifying potential FIE interest in and or targeting of defense-related technology to the Director, DCHC.

c. DoD Components authorized to engage in RDA who lack a CI analytical element may request assistance from the designated MDCO in accordance with Reference (v). If a supporting MDCO is not designated, the DoD Component requests support from the Director, DCHC.

3. ANALYSIS OF FOREIGN COLLECTION THREATS TO RDA PROGRAMS WITH CPI. The identification of CPI in an RDA program requires analytical support from the supporting Defense CI Component. To initiate analytical support, the RDA program manager or designee requests analysis of foreign collection threats from the supporting Defense CI Component in accordance with Reference (d). The supporting Defense CI Component:

a. Determines if analysis is likely to add actionable information to known FIE collection capabilities, methods of operation, or need for program-related or defense-related technology, or CPI. If additional analysis will not add actionable information, assistance is provided to the requesting RDA program manager to obtain existing IC threat assessments or related products pertaining to foreign collection threats for program protection planning purposes.

b. Gathers programmatic information necessary to aid the analytical process. If the analytical effort is deemed appropriate:

(1) Coordinates with the Director, DIA, for production of a TTRA. The TTRA shall serve as a basis for CI analysis.

(2) Completes CI analysis and merges the TTRA with the appropriate CI analytical product. Provides the single-source document to the requesting RDA program manager.

(3) Validates the currency and relevancy of intelligence and CI analytical products used to assess the foreign collection threat and referenced in a PPP prior to major milestone decisions, when requested by an RDA program manager or MDA, or at least every 3 years.

(4) Certifies, in writing, that the product is current; if not current, updates the product or initiates a new analytical effort.

4. THREAT ANALYSIS OF SUPPLY CHAIN RISK. Defense Intelligence Components follow guidance established in Director of Central Intelligence Directive (DCID) 7/6 (Reference (aj)) for all-source threat analysis supporting risk mitigation of intelligence-related acquisitions. DoD Components that are not IC members shall coordinate with the Director, DCHC, for all-source threat analysis of supply chain risk for RDA programs.

a. In support of the DoD SCRM process, the Director, DCHC:

(1) Manage production of threat analysis of supply chain risk in accordance with National Security Presidential Directive-54/Homeland Security Presidential Directive-23 and implementation of the U.S. Government-wide Cyber Counterintelligence Plan (References (ak) and (al)) and Reference (e).

(2) (U//FOUO) Conduct threat analysis of supply chain risk focusing on identifying foreign-affiliated capabilities or activities that would enable an adversary to exploit

vulnerabilities, maliciously modify a provided product or service, sabotage system function, or clandestinely extract data or information.

(3) (U//FOUO) Collaborate with IC elements conducting supply chain threat analysis and incorporate tactics, techniques, and procedures appropriate to the DoD into the DCHC Threat Analysis Center (TAC) methodology to ensure consistency of practice across the IC.

(4) Establish agreements with the DoD Components for threat analysis of supply chain risk.

(5) Collect, retain, and disseminate supply chain threat analysis products in accordance with DoD 5240.1-R (Reference (am)). Safeguard classified and sensitive information in threat analysis products in accordance with DCID 6/6, DoDI 5200.01, DoD 5200.1-R, and DoD 5220.22-M (References (an), (ao), (ap), and (aq)).

(6) Develop and design threat analysis products to inform and support DoD acquisition mitigations and risk management options, in support of comprehensive SCRM programs and activities. Products accomplished in support of SCRM are exempt from sections 2 and 15 of Enclosure 3 in Reference (ai).

(7) Inform the authorized DoD OFCO elements of entities posing a significant threat to the RDA supply chain and provide threat analysis products to the Defense CI Component supporting the requesting RDA program.

(8) Coordinate requests for threat analysis in support of SCRM requirements with the Cognizant Security Agency (e.g., the Director, DSS) for National Industrial Security Program cleared companies.

(9) Collaborate with the USD(AT&L), ASD(NII)/DoD CIO, and the DoD RDA Components to develop and deliver training for the acquisition workforce, CDCs, intelligence, security, and CI personnel with emphasis on the threat, vulnerabilities, and risks to the supply chain.

(10) (U//FOUO) Annually, and in collaboration with relevant IC elements, produce a strategic assessment illustrating foreign threats to the RDA supply chain to include methods of operation, indicators of supply chain threat, and incorporate, when feasible, case studies of supply chain incidents.

b. DoD Components requesting threat analysis of supply chain risk from the TAC shall implement measures to safeguard information in threat analysis products in accordance with subparagraph 4.a.(5) of this appendix. The SCRM focal point shall ensure that DoD personnel (non IC or CI):

(1) Are cleared to access information up to Top Secret and eligible for access to Sensitive Compartmented Information.

(2) Require access to TAC threat analysis products to perform a lawful government function; and have executed a confidentiality agreement. The Component SCRM focal point shall maintain the confidentiality agreements and provide them to the TAC upon request.

(3) Not disseminate U.S. person information in threat analysis products outside the approved members of the SCRM focal point without the prior approval of the TAC. Persons that the SCRM focal point expects to need recurring access to TAC threat analysis products shall meet the requirements in subparagraph 4.b.(2) of this appendix.

(4) Are contractors providing system engineering services or advice and assistance to the SCRM focal point or support the RDA program under a contract that avoids or mitigates organizational conflict of interest as provided for in the Federal and defense acquisition rules.

c. The SCRM focal point shall inform the TAC when a breach of confidentiality occurs with periodic updates on the status of an inquiry until final disposition.

APPENDIX 2 TO ENCLOSURE 3

CISP

1. GENERAL. The Defense CI Components use a CISP to integrate CI activities into RDA, manage, and document non-investigative or non-operational activities conducted. A CISP:

a. Is prepared by the MDCO designated by Reference (v) when required for a Combatant Command.

b. May be appended to a PPP or made available for review by an MDA when requested.

c. Takes precedence over a CI Coverage Plan at supported locations when such a plan is required in accordance with DoDI 5240.19 (Reference (ar)).

d. Is classified in accordance with DoDI S-5240.08 (Reference (as) and the cognizant program security classification guide.

e. Is coordinated with:

(1) RDT&E directors, Component UARC manager(s), RDA program manager(s), or equivalent representative(s).

(2) The DSS and the facility security officer for CISPs supporting a CDC. Provide the supporting DSS CI field office with a copy of the CISP developed for CDCs with CPI.

2. REQUIREMENTS. The Defense CI Components implement a CISP in support of:

a. RDA programs with CPI.

b. DoD Component-designated RDT&E facilities.

c. CDCs considered essential by an RDA program manager and where CPI is present.

3. ELEMENTS OF A CISP. A CISP, at a minimum, addresses three primary areas:

a. Description of the Facility, RDA Program with CPI, or a CDC with CPI. The implementing CI Component, at their discretion, may develop a CISP encompassing all RDA programs with CPI under the cognizance of an RDT&E facility, under the cognizance of a Program Executive Office, or for essential CDCs supporting the facility or RDA program where CPI is present.

(1) Provide contact information for key management personnel (i.e., Program Manager, Facility Security Officer, RDT&E site director, Facility Security Officer).

(2) Include the commercial and government entity code for defense industry and CDCs affiliated with the supported facility or RDA program with CPI.

(3) Identify all RDA programs with CPI. Create an annex for those RDA programs, facilities, and CDCs when the CI activities are unique or cannot be adequately addressed by an overarching CISP.

(4) Identify other activities that support the facility or program to accomplish its mission (e.g., defense industry contractors, academic institutions, FFRDCs, UARCs, or test and evaluation centers – domestic and foreign).

b. Activities Determination. CI activities in a CISP are based on an assessment of the foreign collection threat, the relationship between threat and vulnerabilities, and are selected to detect FIE-associated activity. CI activities identified in Enclosure 3, paragraph 3.b, form the foundation for CI support, and:

(1) Specify the CI activity that will occur; when the activity will be conducted, and the assistance needed from the supported facility, program, or CDC.

(2) Are reviewed with the organization's security element or the security element supporting program protection. This increases efficiency of the PPP, as well as other security-related actions at RDT&E facilities or CDCs.

c. Signature. At a minimum, the CISP is signed by the senior CI person representing the implementing Defense CI Component.

4. REVIEW AND ARCHIVING. CISPs are:

a. Reviewed at least annually and updated as threat conditions change, or the nature of the CI activities conducted are substantially revised.

b. Provided to the gaining Defense CI Component upon transition from research to development to acquisition to deployment.

c. In effect until the supported RDT&E facility no longer engages in R&E or technology development activities.

d. Retired and archived when the CPI is demilitarized or when the RDA proponent determines a CISP is no longer required.

ENCLOSURE 4

COORDINATING CI SUPPORT

1. GENERAL. RDA program personnel appointed to coordinate CI activities supporting RDA programs shall:

a. Incorporate provisions enabling the Defense CI Component to support essential CDCs into the PPP, the DD Form 254, "DoD Contract Security Classification Specification," or associated contractual instruments, as appropriate.

b. Request assistance in obtaining intelligence assessments and CI analytical products that describe foreign collection threats to defense-related technology. RDA program personnel review products to determine if they meet the requirements for protection of RDA programs before requesting new production.

c. Request threat analysis of supply chain risk from the Director, DCHC, in accordance with section 4 of Appendix 1 to Enclosure 3.

d. Request analysis of foreign collection threats to RDA programs with CPI in accordance with section 3 of Appendix 1 to Enclosure 3.

e. Involve Defense CI Component personnel in technology protection, CPI identification, or intelligence support working groups.

f. Annotate, in the PPP, analytical products used to assess foreign collection threats to RDA programs with CPI.

2. COORDINATING CI SUPPORT. To initiate and coordinate CI activities supporting RDA programs, the RDA official shall inform the supporting Defense CI Component of:

a. RDT&E facilities and CDCs considered essential to the RDA effort.

b. Planned test or evaluation to occur at a foreign-owned and/or operated test facility, or at a U.S. Government or commercially owned or operated test facility when it is anticipated that foreign nationals may attend or may be provided with the results of such tests or evaluations.

c. Planned or ongoing FMS where CPI may be transferred.

d. The development, testing, procurement, production of systems with CPI from acquisition to fielding, to include those transferred from a special access program to collateral status.

e. Suspected or confirmed loss or compromise of CPI, or a breach of anti-tamper protection.

f. Foreign military or affiliated personnel participating in a foreign visit and assignment program, or engaged in training and education programs.

g. Requests for information from entities, persons, businesses (foreign or domestic) not associated with the RDA program for CPI-related information or a request to export or transfer CPI/defense-related technology that has not been coordinated with or concurred with by the RDA program manager.

h. RDA program personnel with access to CPI.

i. Known or suspected compromise of IT systems affecting the RDA program in accordance with Reference (ad).

ENCLOSURE 5

CI RDA IMG CHARTER

1. PURPOSE. The Defense CI RDA IMG is the principal forum for coordinating and sharing RDA information among the Defense CI Components.

2. MEMBERSHIP. The CI RDA IMG shall by chaired by the Director, DCHC. Primary membership consists of representatives from DCHC RDA functional management element, OFCO and analytical elements, the office of the USD(I), the MDCOs, DSS CI, USSOCOM CI element, Defense Agency CI elements, and the DIA Defense Warning Office. The Chair may expand membership to include full-time or permanent part-time Federal employees from other DoD or Federal organizations. Military Service members shall be active duty personnel or members of the Reserve or National Guard Components in positions authorized in accordance with Reference (u).

3. MEETINGS. The CI RDA IMG shall convene quarterly. The Chair may meet by video teleconference or other means.

4. ACTIVITIES. The CI RDA IMG shall:

a. Identify and share information on activities that support RDA programs.

b. Exchange information on foreign intentions, collection capabilities, and activities targeting U.S. technology.

c. Discuss and coordinate CI activities supporting RDA special projects and other initiatives. The Chair may establish sub-groups to accomplish assigned projects and actions.

d. Coordinate and deconflict CI activities supporting RDA responsibilities between and among supporting CI organizations.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASIC	application-specific integrated circuit
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
CDC	cleared defense contractor
CFR	Code of Federal Regulations
CI	counterintelligence
CI RDA IMG	Counterintelligence Research, Development, and Acquisition Integrated Management Group
CISP	counterintelligence support plan
CPI	critical program information
DCHC	Defense Counterintelligence and Human Intelligence Center
DSCA	Defense Security Cooperation Agency
DIA	Defense Intelligence Agency
DLA	Defense Logistics Agency
DoDD	DoD Directive
DoDI	DoD Instruction
DPEP	defense personnel exchange program
DSS	Defense Security Service
DUSD(I&S)	Deputy Under Secretary of Defense for Intelligence and Security
EEUM	enhanced end use monitoring
EAR	Export Administration Regulation
FBI	Federal Bureau of Investigation
FFRDC	Federally Funded Research and Development Center
FIE	foreign intelligence entity
FMS	foreign military sales
HUMINT	human intelligence
IC	intelligence community
IMG	Integrated Management Group
IT	information technology
MAC	mission assurance category
MDA	milestone decision authority
MDCO	Military Department Counterintelligence Organization
PPP	Program Protection Plan

R&E	research and engineering
RDA	research, development, and acquisition
RDT&E	research, development, test, and evaluation
SCRM	supply chain risk management
TAC	Threat Analysis Center
TSC	trade security control
TTRA	technology targeting risk assessment
UARC	University Affiliated Research Center
USML	United States Munitions List
U.S.C.	United States Code
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
USSOCOM	United States Special Operations Command

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

acquisition. The conceptualization, initiation, design, development, test, contracting, production, deployment, logistics support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in or in support of military missions.

applied research. Defined in Volume 2B, Chapter 5, Section 050201 of DoD 7000.14-R (Reference (at)).

basic research. Defined in Reference (at).

CDC. A company or academic institution (i.e., university or college) that has entered into a security agreement with the DoD, and was granted a facility (security) clearance enabling the entity to be eligible for access to classified information of a certain category, as well as all lower categories.

CI activities. Defined in Reference (b).

CI functional services. Activities engaged in by personnel trained in CI and conducted to detect espionage, sabotage, terrorism, or related intelligence activities of an FIE directed against the DoD, and that enable one or more of the CI functions (investigations, collection, operations, or analysis and production).

CISP. A formal and living plan describing activities conducted by a Defense CI Component in support of a DoD RDA program or activity with CPI, at DoD-affiliated RDT&E facilitates, and at essential CDCs where CPI resides.

Component Acquisition Executive. The single official within a DoD Component that is responsible for all acquisition functions within that component. This includes Service Acquisition Executives for the Military Departments and acquisition executives in other DoD Components, such as the USSOCOM and DLA, who have acquisition management responsibilities.

computer network attack. Defined in Joint Publication 1-02 (Reference (au).

computer network exploitation. Defined in Reference (au).

contracted fundamental research. Defined in Reference (l).

covered system. All DoD critical information systems and weapons systems, which includes major systems as defined by section 2302(5) of Reference (u); national security systems as defined by section 3542 of title 44, U.S.C. (Reference (av)); and all DoD information systems, categorized as Mission Assurance Category (MAC) I, and select DoD information systems categorized as MAC II, in accordance with DoDD 8500.01E (Reference (aw)).

CPI. Defined in Reference (d).

critical component. A subsystem, assembly, or component of a system that itself delivers mission-critical functionality to the system, or that may, by virtue of system design, expose vulnerability in the mission-critical functions of other components within the system.

critical foreign military need. Defense-related technology identified by intelligence analysis of foreign science and technology requirements that could significantly enhance foreign military capability; is restricted for export or transfer under U.S. law to a foreign entity; and would require a foreign entity to use improper methods to acquire.

cyber intrusion damage assessment. Defined in Reference (ad).

defense articles and services. Defined in Reference (c).

Defense CI Component. Defined in Reference (a).

defense industry. Comprises government and commercial industry involved in research, development, production, and service of military material, equipment, and facilities. Within the context of this Instruction, the term does not include a CDC.

Defense Intelligence Component. Defined in Reference (a).

defense-related technology. Information and technology developed for, utilized in, or integrated into a military system. Defense-related technology is:

Export-controlled as specified in parts 120.6, 120.9, and 121.1 of title 22, Code of Federal Regulations (CFR), also known as the "United States Munitions List (USML)" (Reference (ax)).

Export-controlled as specified in part 774 of title 15, CFR, also known as the "Commerce Control List in the Export Administration Regulations (EAR)" (Reference (ay)).

Emerging or developing, and not characterized as fundamental or contracted fundamental research, and that putatively, when complete will produce a defense article or defense service, including its underlying technology and software, which would be covered by the USML, or a dual-use article, including its underlying technology and software, which would be covered by the EAR in explicit terms, i.e., other than via EAR99.

Additional information, definitions, and descriptions can be found in References (c), (ae), and DoDI 5230.25 (Reference (az)).

direct commercial sale. Defined in Reference (i).

DPEP. Defined in Reference (n).

EEUM. Defined in Reference (i).

FFRDC. Research and development-performing organizations that are exclusively or substantially financed by the Federal Government and are supported by the Federal Government either to meet a particular research and development objective or, in some instances, to provide major facilities at either universities or corporate or contractor locations for applied research or development purposes.

FIE. Defined in Reference (au).

FMS. Defined in Reference (i).

foreign collection threat. Opportunity for a foreign entity or cooperating DoD personnel (an insider) to overtly, covertly or clandestinely collect information about RDA programs, technologies, system capabilities and employment methods that may enable an adversary to copy, counter, or defeat a capability, or inhibit, exploit, or sabotage a defense system. Within the context of this Instruction, the term collectively refers to threats posed by or from an insider, cyber exploitation, supply chain manipulation, an FIE, a foreign company, international transfers or exports of technology, and disposal of export-controlled technology.

fundamental research. Defined in Reference (k).

information and communication technology (ICT). Includes but is not limited to information technology as defined in section 11101 of title 40, U.S.C. (Reference (ba)). The term reflects the

convergence of information technology and communications. ICT includes all categories of ubiquitous technology used for gathering, storing, transmitting, retrieving, or processing information (e.g., computing systems, software, mobile telephony, satellite communications, and networks).

IT. Defined in Reference (t)).

IT architecture. Defined in Reference (t).

MDA. Defined in Reference (h).

MDCO. Elements of the Military Departments authorized to conduct CI investigations and OFCO, i.e., Army CI, Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

OFCO. Defined in Reference (t).

operational support package. Defined in Reference (ai).

PPP. Defined in Reference (d).

R&E. Defined in Reference (e).

RDA. All activities associated with research and engineering, acquisition, international transfers of technology, and disposal of defense-related technology.

RDA program. A directed, funded effort, inclusive of DoD research and engineering activities or an acquisition program that provides a new, improved, or continuing materiel, weapon, or information system or service capability in response to an approved need.

RDA program manager. Designated individual within a research and engineering program, project, or acquisition program with responsibility for and authority to accomplish technology or program objectives for research, development, production, and sustainment to meet the user's operational needs.

RDT&E facility. A DoD, Federal agency, CDC, or academic installation or site housing one or more DoD RDT&E organizations or performing R&E activities on behalf of the Department of Defense. Examples include installations; UARCs, FFRDCs, laboratories; research, development, and engineering centers; warfare centers; test centers, ranges, or arsenals or proving grounds.

risk assessment for technology transfer. Assessment of the risk that U.S. technology shared with a given country—through defense-related trade or cooperation—will be exploited or retransferred without authorization. This includes detailed analysis of: export controls and export control enforcement capabilities; participation in international nonproliferation efforts; involvement in diversion and transshipment of U.S. technology; counterintelligence capabilities;

arms trade; defense technology cooperation; third-country intelligence presence; intelligence collection against U.S. technology; and reverse-engineering capabilities.

SCRM. The management of supply chain risk whether presented by the supplier, the supplied product and its sub-components, or the supply chain (e.g., packaging, handling, storage, and transport).

supply chain risk. The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, otherwise degrade the function, use or operation of the item or system.

technology. Defined in Reference (c).

disruptive technology. Technology is disruptive if it will counter U.S. technological superiority or significantly affect U.S. military forces, economic power, critical infrastructure, or national security interests (Reference (af)).

emerging technology. Technology is emerging if it has attained technology readiness level 4 (component and/or breadboard validation in laboratory environment) as described in the Technology Assessment Deskbook (Reference (bb)).

enabling technology. Technology is enabling because the problems posed are particularly difficult and solutions require a much higher degree of technical sophistication and experience.

TSC. Defined in Reference (j).

TTRA. Defined in Reference (d).

UARC. Part of a university or college that receives sole source (non-competitive funding) contract funding from the DoD in order to establish or maintain an essential engineering, research, and/or developmental capability.