



Department of Defense INSTRUCTION

NUMBER 5205.13
January 29, 2010

ASD(NII)/DoD CIO

SUBJECT: Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities

References: See Enclosure 1

1. PURPOSE. This Instruction establishes policy, assigns responsibilities, and delegates authority in accordance with the authority in DoD Directive (DoDD) 5144.1 (Reference (a)) for directing the conduct of DIB CS/IA activities to protect unclassified DoD information, as defined in the Glossary, that transits or resides on unclassified DIB information systems and networks.
2. APPLICABILITY. This Instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").
3. DEFINITIONS. See Glossary.
4. POLICY. It is DoD policy to:
 - a. Establish a comprehensive approach for protecting unclassified DoD information transiting or residing on unclassified DIB information systems and networks by incorporating the use of intelligence, operations, policies, standards, information sharing, expert advice and assistance, incident response, reporting procedures, and cyber intrusion damage assessment solutions to address a cyber advanced persistent threat.
 - b. Increase DoD and DIB situational awareness regarding the extent and severity of cyber threats in accordance with National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (b)).

c. Create a timely, coordinated, and effective CS/IA partnership with the DIB, developing operating guidance and undertaking activities that:

(1) Maintain a DoD-DIB Collaborative Information Sharing Environment (DCISE), to facilitate DoD coordination of threat information sharing and measures enabling the protection of unclassified DoD information transiting or residing on DIB information systems and networks.

(2) Develop procedures for sharing DoD cyber threat information, unclassified and classified, with the DIB.

(3) Share DoD computer network defense and CS/IA best practices with the DIB.

(4) Develop standard procedures for DIB incident reporting and response.

(5) Develop a mechanism to assist the DIB in conducting self-assessments of CS/IA activities.

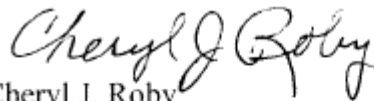
(6) Develop standard procedures for cyber intrusion damage assessment and remediation assistance support to the DIB. Update contracting and acquisition policy and procedures as they relate to CS/IA activities to improve the protection of unclassified DoD information on DIB unclassified information systems and networks.

(7) Adhere to the National Industrial Security Program (NISP) for protection of classified information in the DIB in accordance with DoDD 5220.22 and DoD Manual 5220.22-M (References (c) and (d)).

5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Web Site at <http://www.dtic.mil/whs/directives>.

7. EFFECTIVE DATE. This Instruction is effective immediately.



Cheryl J. Roby
Principal Deputy
Assistant Secretary of Defense for Networks
and Information Integration/ DoD Chief
Information Officer

Enclosures

1. References
 2. Responsibilities
- Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
- (b) National Security Presidential Directive No. 54/Homeland Security Presidential Directive No. 23, "Cybersecurity Policy," January 8, 2008¹
- (c) DoD Directive 5220.22 "National Industrial Security Program," September 27, 2004
- (d) DoD Manual 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006
- (e) DoD Directive 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure," January 14, 2010
- (f) DoD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 20, 2010
- (g) Department of Homeland Security, "National Infrastructure Protection Plan," 2009²
- (h) Department of Defense and Department of Homeland Security, "Defense Industrial Base, Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan," May 2007³
- (i) Deputy Secretary of Defense Memorandum, "Department of Defense Reform Initiative Directive #27 - DoD Computer Forensics Laboratory and Training Program," February 10, 1998
- (j) Deputy Secretary of Defense Memorandum, "Department of Defense Computer Forensics Laboratory (DCFL), and Department of Defense Computer Investigations Training Program (DCITP)," August 17, 2001
- (k) The National Military Strategy for Cyberspace Operations, December 2006⁴
- (l) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended
- (m) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
- (n) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008
- (o) DoD 5200.1-R, "Information Security Program," January 14, 1997
- (p) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008

¹ Copies of this restricted distribution document are available to authorized personnel upon request to DHS.

² Copies of this document are available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

³ Copies of this document are available at <http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf>

⁴ Copies of this classified document are available at <http://www.jtfgno.smil.mil/site/documents/J54/20061201NMS-CO.pdf>

ENCLOSURE 2

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO shall:

a. Oversee DIB CS/IA activities, including related DoD Cyber Crime Center (DC3) activities, and develop and coordinate additional policy guidance consistent with this Instruction.

b. Chair the DIB CS/IA Executive Committee.

c. Coordinate with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) on the incorporation of DIB CS/IA requirements in acquisition programs, contracts, and regulations, and on cyber intrusion damage assessment matters pertaining to the DIB.

d. Coordinate with the Under Secretary of Defense for Intelligence (USD(I)) on intelligence, counterintelligence, security support, and the implementation of information security policy as it relates to DIB CS/IA activities and as it relates to adherence to the NISP.

e. Coordinate with the Under Secretary of Defense for Policy (USD(P)) on integrating DIB CS/IA cyber threat information-sharing activities and enhancing DoD and DIB cyber situational awareness in accordance with Reference (b) and in support of DoDD 3020.40 (Reference (e)).

f. Coordinate with the Inspector General of the Department of Defense (IG DoD) on oversight and policy guidance with respect to audits and criminal investigations relating to DIB CS/IA activities.

g. Coordinate with the Secretary of the Air Force for DC3-related DIB CS/IA activities.

2. USD(I). The USD(I) shall:

a. Serve as the senior DoD intelligence, counterintelligence, and security official responsible for overseeing security policy matters, including personnel, physical, industrial, and information, as well as all source-intelligence and classified threat information sharing related to DIB CS/IA activities.

b. Oversee policy and management of the NISP through the Defense Security Service (DSS) in accordance with Reference (d) and in support of DIB CS/IA activities related to classified information.

c. Coordinate with the ASD(NII)/DoD CIO on implementation of information security policy as it relates to DIB CS/IA activities.

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

a. Ensure that cleared contractors receiving classified information through DIB CS/IA activities have security programs that comply with applicable NISP requirements.

b. Collaborate with DC3 on the evaluation and analysis of the cyber threat information received from and provided to cleared contractors receiving classified information through DIB CS/IA activities.

4. DIRECTOR, NATIONAL SECURITY AGENCY (NSA). In addition to the responsibilities outlined in section 11 of this enclosure, and in accordance with Reference (b) and DoDD 5100.20 (Reference (f)), the Director, NSA, under the authority, direction, and control of the USD(I), shall provide support to the DCISE and cyber intrusion damage assessment analysis as part of DIB CS/IA activities.

5. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). In addition to the responsibilities outlined in section 11 of this enclosure, the Director, DIA, under the authority, direction, and control of the USD(I), shall provide support to the DCISE and cyber intrusion damage assessment analysis as part of DIB CS/IA activities.

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

a. Identify, develop, update, and implement policy and processes into the DoD acquisition contracting process for improved protection of unclassified DoD information transiting or residing on unclassified DIB information systems and networks as part of DIB CS/IA activities.

b. Develop cyber intrusion damage assessment policy and oversee the process to conduct assessments of DoD programs, as required, on unauthorized access and potential compromise of unclassified DIB information systems and networks containing unclassified DoD information.

7. IG DoD. The IG DoD shall provide oversight and policy guidance with respect to criminal investigations in support of DIB CS/IA activities.

8. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE (GC, DoD). The GC, DoD, shall provide advice regarding all legal matters and services relating to DIB CS/IA

activities and provide representatives to DIB CS/IA committees and working groups, as necessary.

9. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER (CFO), DEPARTMENT OF DEFENSE (USD(C)/CFO). The USD(C)/CFO shall monitor DoD Component budgets related to DIB CS/IA activities to ensure resulting costs are resourced.

10. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND AMERICAS' SECURITY AFFAIRS (ASD(HD&ASA)). The ASD(HD&ASA), under the authority, direction, and control of the USD(P), shall:

a. Integrate DIB CS/IA activities in support of Reference (b) into the Defense Critical Infrastructure Program (Reference (e)).

b. Coordinate assigned Sector-Specific Agency responsibilities pertaining to DIB CS/IA activities with the USD(AT&L) and ASD(NII)/DoD CIO, as appropriate, in accordance with the Department of Homeland (DHS) Security National Infrastructure Protection Plan and the DoD and DHS Defense Industrial Base, Critical Infrastructure and Key Resources Sector-Specific Plan (References (g) and (h)).

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

a. Support DIB CS/IA activities as appropriate in accordance with public law and DoD policy and consistent with their assigned missions, and shall plan, program, resource, and budget for costs associated with implementing this policy.

b. Ensure acquisition programs support DIB CS/IA activities in accordance with public law and acquisition regulations.

c. Based on USD(AT&L) policy guidance, develop procedures and conduct cyber intrusion damage assessments in support of DIB CS/IA activities to determine the overall impact of the exfiltration or modification of data on current and future weapons programs, scientific and research projects, and warfighting capabilities stemming from unauthorized intrusions into DIB unclassified information systems.

12. SECRETARY OF THE AIR FORCE. In addition to the responsibilities in section 11 of this enclosure, the Secretary of the Air Force, as the DoD Executive Agent (EA) for DC3 digital forensic training and laboratory services in accordance with the Deputy Secretary of Defense Memorandums (References (i) and (j)), shall support DIB CS/IA activities.

13. DIRECTOR, DC3. The Director, DC3, under the authority, direction, and control of the Secretary of the Air Force, as the DoD EA, shall:

a. Provide hosting services for the DCISE to facilitate DoD coordination of threat information sharing and measures enabling the protection of unclassified DoD information transiting or residing on DIB information systems and networks.

b. Serve as the DoD operational focal point for DIB CS/IA threat information sharing through the DCISE.

c. Implement DoD policies, processes, and standards pertaining to DIB cyber security activities, forensics analysis, and training; provide support to the Intelligence Community, other DoD Components, and DoD law enforcement elements related to DCISE operations.

d. Implement and oversee standard operating procedures for DIB incident reporting and response.

e. Support DIB CS/IA activities by leveraging the Defense Computer Forensics Laboratory, the Defense Cyber Crime Institute, and the Defense Cyber Investigations Training Academy and the presence of the National Cyber Investigative Joint Task Force/Analytical Group hosted at DC3 in accordance with References (i) and (j).

14. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. In addition to the responsibilities in section 11 of this enclosure, the Chairman of the Joint Chiefs of Staff shall:

a. Ensure joint training, plans, and operations are consistent with DIB CS/IA activities.

b. Ensure Combatant Commander DIB cyber security requirements are integrated into DIB CS/IA activities.

c. Evaluate, as part of DIB CS/IA cyber intrusion damage assessment activities, the impact on warfighting capabilities resulting from the loss of DoD information due to intrusions into DIB unclassified information systems and networks.

d. Oversee tasks relating to DIB CS/IA activities implementation in National Military Strategy for Cyberspace Operations (Reference (k)).

15. COMMANDER, UNITED STATES STRATEGIC COMMAND (CDRUSSTRATCOM).

In addition to the responsibilities in section 11 of this enclosure, the CDRUSSTRATCOM, through the Chairman of the Joint Chiefs of Staff, shall support DIB CS/IA activities, including analysis and reporting and cyber intrusion damage assessments, as required.

16. COMMANDER, UNITED STATES JOINT FORCES COMMAND (CDRUSJFCOM). In addition to the responsibilities in section 11 of this enclosure, the CDRUSJFCOM, through the Chairman of the Joint Chiefs of Staff, shall integrate DIB CS/IA activities into joint exercises and training.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
CDRUSJFCOM	Commander, United States Joint Forces Command
CDRUSSTRATCOM	Commander, United States Strategic Command
CS/IA	cyber security/information assurance activities
DC3	DoD Cyber Crime Center
DCIP	Defense Critical Infrastructure Program
DCISE	DoD-DIB Collaborative Information Sharing Environment
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	defense industrial base
DoDD	DoD Directive
DSS	Defense Security Service
EA	Executive Agent
GC DoD	General Counsel of the Department of Defense
IG DoD	Inspector General of the Department of Defense
NISP	National Industrial Security Program
NSA	National Security Agency
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this Instruction.

advanced persistent threat. An extremely proficient, patient, determined, and capable adversary, including two or more of such adversaries working together.

cyber security. Measures taken to protect a computer network, system, or electronic information storage against unauthorized access or attempted access.

cyber intrusion damage assessment. A managed, coordinated, and standardized process conducted to determine the impact on future defense programs, defense scientific and research projects, or defense warfighting capabilities resulting from an intrusion into a DIB unclassified computer system or network.

DIB. Defined in Joint Publication 1-02 (Reference (l)).

information assurance. Defined in DoDD 8500.01E (Reference (m)).

Sector-Specific Agency. Defined in Reference (g).

unclassified DoD information. Unclassified information that requires controls pursuant to DoD Instruction 5200.1, Appendix 3 of DoD 5200.1-R, and DoDD 5230.09 (References (n), (o), and (p)).