Department of Defense

INSTRUCTION

NUMBER 5205.13
January 29, 2010
Incorporating Change 2, August 21, 2019

DoD CIO

SUBJECT: Defense Industrial Base (DIB) Cybersecurity (CS) 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) 5144.02 (Reference (a)) for directing the conduct of DIB CS 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:

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. The United States Coast Guard. The United States Coast Guard will adhere to DoD cybersecurity requirements, standards, and policies in this issuance in accordance with the direction in Paragraphs 4a, b, c, and d of the Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security (Reference (o)).

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 incident 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 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 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 activities.

(6) Develop standard procedures for cyber incident damage assessment and remediation assistance support to the DIB. Update contracting and acquisition policy and procedures as they relate to CS 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 DoD Instruction 5220.22 and DoD Manual 5220.22-M (References (c) and (d)).

5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. **Cleared for public release**. This instruction is available on the Directives Division Website at https://www.esd.whs.mil/DD/.

7. SUMMARY OF CHANGE 2. The changes to this issuance are administrative and update organizational titles and references for accuracy.

8. EFFECTIVE DATE. This Instruction is effective January 29, 2010.

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 5144.02, "DoD Chief Information Officer," November 21, 2014, as amended
(b) National Security Presidential Directive No. 54/Homeland Security Presidential Directive No. 23, "Cybersecurity Policy," January 8, 2008[1]
(c) DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011, as amended
(d) DoD Manual 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended
(e) DoD Directive 3020.40, "Mission Assurance (MA)," November 29, 2016, as amended
(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," 2013[2]
(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 2010[3]
(i) Department of Defense Cyber Strategy, September 2018
(j) Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," as amended
(k) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(l) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended
(m) DoD Manual 5200.01, "DoD Information Security Program," February 24, 2012, as amended
(n) DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019
(o) Memorandum of Agreement Between the Department of Defense and The Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, January 19, 2017[4]

[1] Copies of this restricted distribution document are available to authorized personnel upon request to DHS.
[2] Copies of this document are available at https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf
[3] Copies of this document are available at https://www.dhs.gov/sites/default/files/publications/nipp-ssp-defense-industrial-base-2010-508.pdf
[4] Available at https://dcms.uscg.afpims.mil/Our-Organization/Assistant-Commandant-for-C4IT-CG-6-/The-Office-of-Information-Management-CG-61/Interagency-Agreements/

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CHIEF INFORMATION OFFICER (DoD CIO). The DoD CIO shall:

a. Oversee DIB CS 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 Executive Committee.

c. Coordinate with the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) and the Under Secretary of Defense for Research and Engineering (USD(R&E)) on the incorporation of DIB CS requirements in acquisition programs, contracts, and regulations, and on cyber incident 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 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 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 activities.

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

b. Oversee policy and management of the NISP through the Defense Counterintelligence and Security Agency (DCSA) in accordance with Reference (d) and in support of DIB CS activities related to classified information.

c. Coordinate with the DoD CIO on implementation of information security policy as it relates to DIB CS activities.

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

a. Ensure that cleared contractors receiving classified information through DIB CS 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 activities.

4. DIRECTOR, NATIONAL SECURITY AGENCY (NSA). In addition to the responsibilities outlined in section 12 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 incident damage assessment analysis as part of DIB CS activities.

5. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). In addition to the responsibilities outlined in section 12 of this enclosure, the Director, DIA, under the authority, direction, and control of the USD(I), shall provide support to the DCISE and cyber incident damage assessment analysis as part of DIB CS activities.

6. USD(A&S). In addition to the responsibilities in Section 12 of this enclosure, the USD(A&S) will 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 activities.

7. USD(R&E). In addition to the responsibilities in Section 12 of this enclosure, the USD(R&E) will develop cyber-incident 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.

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

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

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

11. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY (ASD(HD&GS)). The ASD(HD&GS), under the authority, direction, and control of the USD(P), shall:

a. Integrate DIB CS 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 activities with the USD(A&S) and 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)).

12. DoD COMPONENT HEADS. The DoD Component heads shall:

a. Support DIB CS 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 activities in accordance with public law and acquisition regulations.

c. Based on USD(R&E) policy guidance, develop procedures and conduct cyber incident damage assessments in support of DIB CS 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.

13. SECRETARY OF THE AIR FORCE. In addition to the responsibilities in section 12 of this enclosure, the Secretary of the Air Force, as the DoD Executive Agent (EA) for DC3 digital forensic training and laboratory services shall support DIB CS activities.

14. 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 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 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.

15. 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 activities.

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

c. Evaluate, as part of DIB CS cyber incident 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 activities implementation in National Military Strategy for Cyberspace Operations (Reference (i)).

16. COMMANDER, UNITED STATES CYBER COMMAND (CDRUSCYBERCOM). In addition to the responsibilities in section 12 of this enclosure, the CDRUSCYBERCOM, through the Chairman of the Joint Chiefs of Staff, shall support DIB CS activities, including analysis and reporting and cyber incident damage assessments, as required.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(HD&GS)	Assistant Secretary of Defense for Homeland Defense and Global Security
CDRUSCYBERCOM	Commander, United States Cyber Command
CS	cybersecurity
DC3	DoD Cyber Crime Center
DCIP	Defense Critical Infrastructure Program
DCISE	DoD-DIB Collaborative Information Sharing Environment
DCSA	Defense Counterintelligence and Security Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	defense industrial base
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDIN	DoD Information Network
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(A&S)	Under Secretary of Defense for Acquisition and Sustainment
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
USD(R&E)	Under Secretary of Defense for Research and Engineering

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 incident 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 the DoD Dictionary of Military and Associated Terms (Reference (l)).

information assurance. Defined in DoDI 8500.01 (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 Manual 5200.01, and DoD Instruction 5230.09 (References (n), (o), and (p)).