Department of Defense

DIRECTIVE

NUMBER 5505.13E
March 1, 2010

ASD(NII)/DoD CIO

SUBJECT: DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)

References: See Enclosure 1

1. PURPOSE. This Directive:

a. Directs the establishment of DC3 as an entity within the Department of the Air Force and establishes the functions of DC3.

b. Designates the Secretary of the Air Force (SECAF) as EA for DC3, including its subordinate digital and multimedia forensics laboratory services and cyber investigative training services, in accordance with DoD Directive (DoDD) 5101.1 (Reference (a)).

c. Pursuant to section 125 and in accordance with section 376 of title 10, United States Code (U.S.C.) (Reference (b)), establishes DC3 policy and assigns responsibilities for the centralized coordination of cyber investigative training and digital and multimedia forensics, including research, development, test, and evaluation (RDT&E) and collaboration with other U.S. Government and private industry organizations.

d. Incorporates and cancels Deputy Secretary of Defense Memorandums (References (c) and (d)).

2. APPLICABILITY. This Directive 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 (IG DoD), 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 that the DC3 shall:

a. Serve as one of the designated national cyber centers in accordance with National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)).

b. Serve as the DoD Center of Excellence and establish DoD standards for digital and multimedia forensics in coordination with the DoD Components.

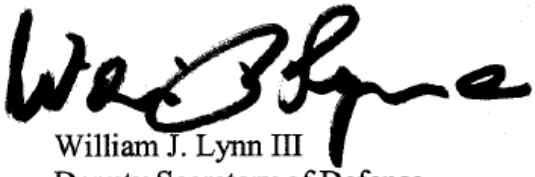
c. Develop and provide specialized cyber investigative training for DoD and non-DoD personnel, as authorized.

d. Serve as the operational focal point for Defense Industrial Base (DIB) cyber security (CS) and information assurance (IA) information sharing and digital forensics analysis activities performed to protect unclassified DoD information -- as defined in the Glossary -- that transits or resides on unclassified DIB information systems and networks.

5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. UNLIMITED. This Directive is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This Directive is effective immediately.



William J. Lynn III
Deputy Secretary of Defense

Enclosures
1. References
2. Responsibilities
3. DC3 Functions

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002
(b) Sections 125 and 376 of title 10, United States Code
(c) Deputy Secretary of Defense Memorandum, "Department of Defense Computer Forensics Laboratory (DCFL), and Department of Defense Computer Investigations Training Program (DCITP)," August 17, 2001 (hereby canceled)
(d) Deputy Secretary of Defense Memorandum, "Department of Defense Reform Initiative Directive #27 – DoD Computer Forensics Laboratory and Training Program," February 10, 1998 (hereby canceled)
(e) National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," January 8, 2008[1]
(f) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
(g) DoD 7000.14-R, "Department of Defense Financial Management Regulations (FMRs)," Volumes 1-15, as amended
(h) DoD Directive 7045.14, "Planning, Programming, and Budgeting System (PPBS)," May 22, 1984
(i) DoD Directive 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure" January 14, 2010
(j) DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005
(k) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(l) DoD Directive O-5240.02, "Counterintelligence," December 20, 2007
(m) DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007
(n) DoD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010
(o) DoD Directive 5220.22, "National Industrial Security Program," September 27, 2004
(p) DoD Instruction 5240.19, "Counterintelligence Support to the Defense Critical Infrastructure Program," August 27, 2007
(q) DoD Directive 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials," January 15, 1986
(r) Sections 1535 and 1536 of title 31, United States Code
(s) Intelligence Community Directive 302, "Document and Media Exploitation," July 6, 2007[2]
(t) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008
(u) DoD 5200.1-R, "Information Security Program," January 1997
(v) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008

[1] Copies of this classified document are available to authorized personnel upon request to DHS.
[2] Copies of this document are available to authorized personnel on the SIPRNET at www.intelink.sgov.gov/wiki/Image:ICD_302.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. Provide overall policy guidance and validated funding and manpower requirements, in coordination with the Under Secretary of Defense for Intelligence (USD(I)), the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the Under Secretary of Defense for Policy (USD(P)), the IG DoD, and the SECAF.

b. Provide guidance and oversight for the EA for DC3 and perform responsibilities as prescribed in paragraph 5.3. of Reference (a).

c. Establish policy and guidance for DC3 activities in accordance with the priorities established by the Secretary of Defense in DoDD 5144.1 (Reference (f)), and in consonance with the USD(I), USD(AT&L), USD(P), IG DoD, and SECAF to ensure the efficient and effective use of DC3 capabilities.

d. Oversee DC3 planning, programming, budgeting, and execution (PPBE) activities by reviewing proposed resource programs and requirements, reviewing budget estimates, approving proposed resource allocations, and monitoring the implementation and performance of approved programs in accordance with the guidance in DoD 7000.14-R (Reference (g)) and the responsibilities in DoDD 7045.14 (Reference (h)). Coordinate with the Heads of the DoD Components, as appropriate, in the development of the DC3 budget requirements.

e. Issue detailed procedural guidance for the DC3 process and timelines associated with the annual DC3 program and budget development, reprogramming, and other PPBE requirements.

f. Approve the addition or deletion of programs, functions, and activities to and from DC3.

g. Coordinate with the USD(AT&L) on programs, policies, and activities pertaining to DC3 involving acquisition, cyber intrusion damage assessment, and digital and multimedia forensics relating to the Defense Forensics Enterprise.

h. Coordinate with the USD(I) on intelligence support and unclassified DoD information as related to DC3 activities.

i. Coordinate with the USD(P) on integrating DC3 activities into the Defense Critical Infrastructure Program (DoDD 3020.40, Reference (i)) and in support of Reference (e) implementation requirements.

j. Coordinate with the Under Secretary of Defense (Comptroller) (USD(C))/Chief Financial Officer (CFO), Department of Defense, on DC3 budget formulation and execution.

k. Coordinate with the IG DoD to ensure appropriate provisioning of DC3 capability to support the criminal investigative requirements of the DoD Components.

l. Coordinate with the SECAF in his or her capacity as the EA for DC3.

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

a. Identify, develop, and implement policy and processes in accordance with DoDD 5134.01 (Reference (j) into DoD acquisition processes for improved protection of unclassified DoD information on DIB information systems and networks, as well as cyber intrusion damage assessments in support of DIB CS and IA activities.

b. In coordination with the ASD(NII)/DoD CIO and the Heads of the DoD Components, develop funding and manpower requirements to support cyber intrusion damage assessments of unauthorized access and potential compromise of unclassified DIB networks containing unclassified DoD information, including forensic and analytic support for DC3.

c. Coordinate with the ASD(NII)/DoD CIO on digital and multimedia forensics relating to the Defense Forensics Enterprise.

3. USD(I). The USD(I) shall oversee the development of intelligence policy, programs, and guidance for DC3 in accordance with DoDD 5143.01 (Reference (k)), DoDD O-5240.02 (Reference (l)), and DoDD 5240.01 (Reference (m)).

4. DIRECTOR, NATIONAL SECURITY AGENCY (NSA)/CHIEF, CENTRAL SECURITY SERVICE (CSS). The Director, NSA/Chief, CSS, under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 11 of this enclosure, shall support DIB CS and IA activities, including DC3 analysis and research, DC3 specialized cyber investigative training, and DC3 digital and multimedia forensic RDT&E, pursuant to DoDD 5100.20 (Reference (n)).

5. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 11 of this enclosure, shall provide analytical support to DC3 activities in support of DIB CS and IA activities and the cyber intrusion damage assessment process.

6. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). The Director, DSS, under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 11 of

this enclosure, shall ensure classified information released to industry by the DC3 through DIB CS and IA activities is properly safeguarded pursuant to DoDD 5220.22 (Reference (o)).

7. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R) shall:

a. Assist the SECAF and the Director, DC3, in developing a DC3 strategic human capital management plan, with supporting recruitment, retention, and development strategies, to ensure DC3 has the talent needed to meet mission requirements.

b. Approve the classification of new positions into the Federal law enforcement job series.

8. USD(C)/CFO. The USD(C)/CFO shall oversee the budget formulation and execution of DC3 activities in the DoD budget in coordination with the ASD(NII)/DoD CIO.

9. IG DOD. The IG DoD, in addition to the responsibilities in section 11 of this enclosure, shall, in coordination with the ASD(NII)/DoD CIO, support DoD Component cyber crime-related criminal investigative requirements.

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 oversee the DoD response to Reference (e) and, in coordination with the ASD(NII)/DoD CIO, integrate the DC3 role in specialized cyber training, in DIB CS and IA activities, and as a national cyber center into the response.

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

a. Provide DC3 funding in accordance with Reference (g) for missions or specialized projects requiring continuing levels of digital and multimedia forensics, investigative training, or other specialized DC3 support or capabilities. The Heads of the DoD Components are encouraged to establish a memorandum of agreement with the Director, DC3, when such requirements arise.

b. Coordinate with the Director, DC3, as the DoD Center of Excellence for digital and multimedia forensics, specialized investigative cyber training and DIB CS and IA activities, including analysis, reporting, and support to cyber intrusion damage assessments.

c. Ensure DoD criminal investigative and counterintelligence (CI) organizations provide DC3, to the maximum extent possible, copies of digital media and logs and investigative and technical data associated with cyber intrusion incidents, investigations, and operations.

12. SECAF. The SECAF, in addition to the responsibilities in section 11 of this enclosure, as the DoD EA for DC3, shall:

a. Establish and maintain DC3 as an entity within the Department of the Air Force with the functions described in Enclosure 3.

b. Provide DC3 funding and manpower in coordination with the ASD(NII)/DoD CIO and the Director, DC3.

c. Assign personnel to DC3 in accordance with approved authorizations and established procedures for detail or assignment to joint duty.

d. Appoint the Director, DC3.

e. Assist the Director, DC3, in developing and executing strategic human capital management plans to ensure DC3 is properly staffed with employees with the requisite skills and competencies needed to perform DC3 mission requirements.

13. COMMANDER, UNITED STATES STRATEGIC COMMAND (CDRUSSTRATCOM). The CDRUSSTRATCOM, in addition to the responsibilities in section 11 of this enclosure, shall coordinate with the ASD(NII)/DoD CIO to support DC3 activities, including analysis and reporting, and shall rely on DC3 for digital and multimedia forensics support and specialized investigative training, as necessary.

ENCLOSURE 3

DC3 FUNCTIONS

1. DIRECTOR, DC3. The Director, DC3, shall:

a. Maintain credentials as a special agent.

b. Plan, program, budget, and execute funding and manpower to accomplish programs and requirements by providing budget estimates, allocating resources, and implementing approved programs consistent with ASD(NII)/DoD CIO and SECAF guidance each fiscal year.

c. Oversee DoD digital and multimedia forensics and cyber investigative processes, procedures, and standards, and support multiple mission areas ranging from criminal investigations, fraud investigations, CI, counterterrorism activities, safety inquiries, and countering threats to critical infrastructure.

d. Communicate directly with the DoD Components on matters related to this Directive. To the extent practicable and consistent with the responsibilities and functions of the Military Departments, the Head of the DoD Component concerned shall be kept informed of such direct communications.

e. Request assistance as needed from other audit, evaluation, and investigative units of the DoD Components. In such cases, assistance shall be requested through the Head of the DoD Component concerned.

f. Pursuant to approved delegations and in accordance with governing regulations, execute hiring authorities and set salary as well as recruitment and retention incentives. Positions assigned to the DC3 may meet requirements for classification as General Series 1811 (Federal Law Enforcement), including coverage under the Federal Law Enforcement Retirement System, subject to approval of the USD(P&R).

2. DC3 FUNCTIONS. The DC3 shall:

a. Function as one of the designated national cyber centers pursuant to Reference (e).

b. Function as the DoD Center of Excellence for digital and multimedia forensics by providing:

(1) Digital and multimedia processing and intrusion analysis for the Department of Defense.

(2) Technical assistance, guidelines, and standards for DoD digital and multimedia forensic organizations, including:

(a) Providing technical assistance to DoD Component digital and multimedia forensic laboratories.

(b) Conducting digital and multimedia forensics analysis for forensic support to CI investigations in accordance with DoD Instruction (DoDI) 5240.19 (Reference (p)).

(c) Maintaining an electronic library of information for test and validation reports for digital forensics tools.

(d) Advancing digital and multimedia forensic RDT&E and collaborating with Government and private industry to keep abreast of cutting-edge technology.

(e) Developing criteria for the referral of media to DC3 by the DoD Components that is the subject of digital and multimedia forensics analysis.

(f) Providing guidance on accreditation of DoD digital forensic labs and training and certification of examiners.

(g) Developing standards for forensic test and validation of cyber investigative and digital forensics hardware and software.

c. Provide specialized investigative training to:

(1) DoD digital forensics examiners, cyber investigators, selected information technology professionals, and other DoD personnel to ensure DoD and DIB information systems are secure from unauthorized use, criminal and fraudulent activities, and foreign intelligence service exploitation; and/or

(2) Personnel responsible for the exploitation of digital media for intelligence and CI objectives.

d. Support digital and multimedia forensic requests from and provide training services to non-DoD Government organizations in accordance with Reference (b), DoDD 5525.5 (Reference (q)), and sections 1535 and 1536 of title 31, U.S.C. (Reference (r)) under a business enterprise and fee-for-service program.

e. Maintain and serve as the operational focal point for threat information sharing through the DoD-DIB Collaborative Information Sharing Environment to protect unclassified DoD information residing on or transiting DIB unclassified networks.

f. Operate as a law enforcement support and CI support activity within the Department of Defense pursuant to the authorities vested in the Secretary of Defense by Reference (b). Unless otherwise directed by the Secretary of Defense, the law enforcement responsibilities assigned by this Directive do not replace or supersede those responsibilities currently assigned to the Defense Criminal Investigative Service, the Army Criminal Investigation Command, the Naval Criminal

Investigative Service, or the Air Force Office of Special Investigations as defense criminal investigative organizations, nor do they supersede the CI authorities of other DoD Components.

g. Seek and maintain, as appropriate, accreditation or certification of DC3 entities, as well as personnel in coordination with the USD(P&R), to the extent such is supportive of and consistent with mission requirements; leverage, as appropriate, inter-agency efforts in this regard.

h. Support DoD critical infrastructure protection by enhancing the cyber security of the DIB against cyber threats and crimes pursuant to Reference (i).

i. Maintain a central clearinghouse and repository for cyber CI tools, techniques, or other procedures and share them with other DoD CI components.

j. Act as a National Media Exploitation Center forensics partner, providing digital forensics processing and analysis for seized digital media to enable multi-disciplinary exploitation objectives, pursuant to Intelligence Community Directive 302 (Reference (s)).

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
CDRUSSTRATCOM	Commander, United States Strategic Command
CI	counterintelligence
CS	cyber security
CSS	Central Security Service
DC3	DoD Cyber Crime Center
DIA	Defense Intelligence Agency
DIB	Defense Industrial Base
DoDD	DoD Directive
DoDI	DoD Instruction
DSS	Defense Security Services
EA	Executive Agent
IA	information assurance
IG DoD	Inspector General of the Department of Defense
NSA	National Security Agency
PPBE	planning, programming, budgeting, and execution
RDT&E	research, development, test, and evaluation
SECAF	Secretary of the Air Force
U.S.C.	United States Code
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
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

PART II. DEFINITIONS

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

CS. Measures taken to protect a computer, networks, or information or computer system (as on the Internet) and electronic information storage facilities belonging to, or operated by or for, the Department of Defense or U.S. Government, against unauthorized access, attack, or attempts to 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. The Department of Defense, the U.S. Government, and private sector worldwide industrial complex with capabilities to perform research and development and to design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

digital evidence. Information of probative value stored or transmitted in binary form.

digital forensics. In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony. Beyond traditional legal purposes, the same techniques, scientific rigor, and procedural precision now support the range of military operations and courses of action (e.g., computer network operations as well as CI objectives).

unclassified DoD information. Unclassified information that requires controls pursuant to DoDI 5200.1, Appendix 3 of DoD 5200.1-R, and DoDD 5230.09 (References (t), (u), and (v)).