

SECRET



Department of Defense INSTRUCTION

NUMBER S-5240.23

December 13, 2010

USD(I)

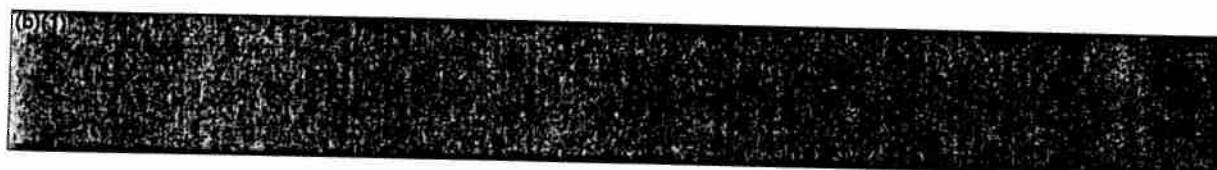
SUBJECT: Counterintelligence (CI) Activities in Cyberspace (U)

(U) References: See Enclosure 1

1. (U) PURPOSE. This Instruction establishes and implements policy and assigns responsibilities for CI activities in cyberspace pursuant to Executive Order 12333 (Reference (a)) and the U.S. Government-Wide Cyber CI Plan (Reference (b)) in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (c)) and DoDD O-5240.02 (Reference (d)) and cancels Under Secretary of Defense for Intelligence (USD(I)) Memorandum (Reference (e)).

2. (U) APPLICABILITY

a. (U) 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. (U) DEFINITIONS. See Glossary.

4. (U) POLICY. It is DoD policy that CI activities in cyberspace shall:

a. (U) Be directed against foreign intelligence services and international terrorist organizations, hereafter referred to as "foreign intelligence entities (FIEs)", in accordance with the mission areas in Reference (d).

Classified by: DoD Instruction C-5240.08

Reason: 1.4(a)

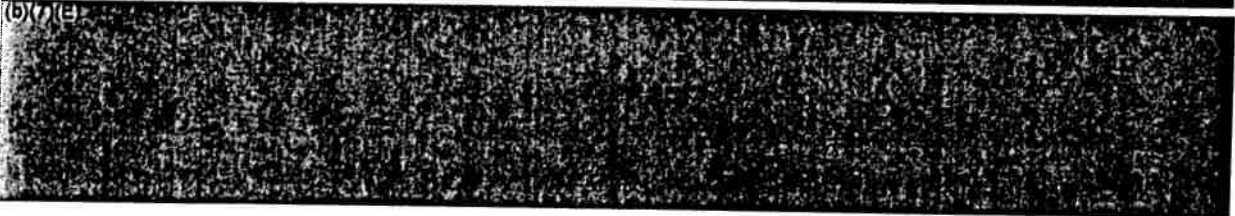
Declassify on: 1 October 2035

SECRET

(b)(7)(E)



(b)(7)(E)



d. (U) Be conducted by technically trained and certified personnel in accordance with Enclosures 2 and 3 of this Instruction.

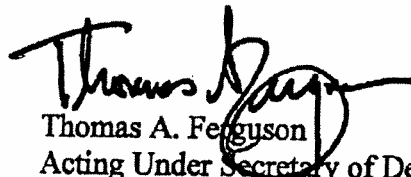
e. (U) Be conducted in accordance with applicable statutes, Reference (c), the Intelligence Oversight procedures listed in DoDD 5240.01 and DoD 5240.1-R (References (g) and (h)) and the privacy program in DoD 5400.11-R (Reference (i)).

5. (U) RESPONSIBILITIES. See Enclosure 2.

6. (U) PROCEDURES. See Enclosure 3.

7. (U) RELEASABILITY. RESTRICTED. This Instruction is approved for restricted release. Authorized users may obtain copies on the SECRET Internet Protocol Router Network from the DoD Issuances Website at <http://www.dtic.smil.mil/whs/directives>.

8. (U) EFFECTIVE DATE. This Instruction is effective upon its publication to the DoD Issuances Website.


Thomas A. Ferguson
Acting Under Secretary of Defense
for Intelligence

- (U) Enclosures
1. (U) References
 2. (U) Responsibilities
 3. (U) Procedures
- (U) Glossary

SECRET

DoDI S-5240.23, December 13, 2010

TABLE OF CONTENTS

(U) The information in this Table of Contents is UNCLASSIFIED.

ENCLOSURE 1: REFERENCES.....4

ENCLOSURE 2: RESPONSIBILITIES.....5

 USD(I).....5

 DEPUTY UNDER SECRETARY OF DEFENSE FOR HUMAN INTELLIGENCE
 (HUMINT), CI, AND SECURITY (DUSD(HCI&S)).....5

 DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY
 SERVICE (DIRECTOR, NSA/CHIEF, CSS)5

 DIRECTOR, DCHC6

 ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND
 INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER
 (ASD(NII)/DoD CIO).....6

 HEADS OF DoD COMPONENTS WITH DEFENSE CI COMPONENTS7

 HEADS OF DoD COMPONENTS WITHOUT DEFENSE CI COMPONENTS7

 COMMANDER, USCYBERCOM.....8

 DIRECTOR, DC38

ENCLOSURE 3: PROCEDURES.....9

 GENERAL.....9

 CI SUPPORT TO CYBERSPACE OPERATIONS.....9

 DoD CI COLLECTION IN CYBERSPACE.....11

 OFCO IN CYBERSPACE.....12

GLOSSARY14

 ABBREVIATIONS AND ACRONYMS.....14

 DEFINITIONS.....15

TABLE


 Indicators of Potential Threat Activity on DoD Networks10

SECRET

DoDI S-5240.23, December 13, 2010

ENCLOSURE 1

REFERENCES (U)

- (a) (U) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
- (b) (U) The National Counterintelligence Executive, "The United States Government-Wide Cyber Counterintelligence Plan 2008," November 25, 2008¹
- (c) (U) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),¹" November 23, 2005
- (d) (U) DoD Directive O-5240.02, "Counterintelligence," December 20, 2007
- (e) (U) USD(I) Memorandum, "Deconfliction of DoD Counterintelligence Cyber Operations with the Intelligence Community," February 2, 2007 (hereby cancelled)
- (f) (U) Trilateral Memorandum of Agreement Among the Department of Defense, the Department of Justice, and the Intelligence Community Regarding Computer Network Attack and Computer Network Exploitation Activities, May 9, 2007¹
- (g) (U) DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007
- (h) (U) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982
- (i) (U) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (j) (U) Under Secretary of Defense for Intelligence Publication, "The DoD Strategy for Counterintelligence in Cyberspace," August 28, 2009¹
- (k) (U) DoD Instruction S-5240.17, "Counterintelligence Collection (U)," January 12, 2009
- (l) (U) DoD Instruction S-5240.09, "Offensive Counterintelligence Operations (OFCO) (U)," October 29, 2008
- (m) (U) DoD Directive S-5105.61, "DoD Cover and Cover Support Activities (U)" May 6, 2010¹
- (n) (U) DoD Directive 5505.13E, "DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)," March 1, 2010
- (o) (U) DoD Instruction 3305.11, "DoD Counterintelligence (CI) Training," March 19, 2007
- (p) (U) DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010
- (q) (U) DoD Instruction 5240.04, "Counterintelligence (CI) Investigations," February 2, 2009
- (r) (U) DoD Directive 3600.01, "Information Operations (IO)," August 14, 2006
- (s) (U) DoD Instruction 5240.6, "Counterintelligence (CI) Awareness, Briefing, and Reporting Programs," August 7, 2004
- (t) (U) DoD Instruction 5240.10, "Counterintelligence Support to the Combatant Commands and the Defense Agencies," May 14, 2004
- (u) (U) DoD Instruction O-5240.21, "Counterintelligence (CI) Inquiries," May 14, 2009
- (b)(1) 
- (w) (U) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition

¹ Available upon request from the Counterintelligence Directorate, DUSD(HCI&S)/CI, Room 3C1088, 5000 Defense Pentagon, Washington, D.C. 20301-5000

SECRET

DoDI S-5240.23, December 13, 2010

ENCLOSURE 2

RESPONSIBILITIES (U)

1. (U) USD(I). The USD(I) shall:

a. (U) Oversee the development and implementation of DoD policy for CI activities in cyberspace.

b. (U) Oversee the development and implementation of the DoD Strategy for CI in Cyberspace (Reference (j)).

c. (U) Approve training and certification standards for CI activities in cyberspace.

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

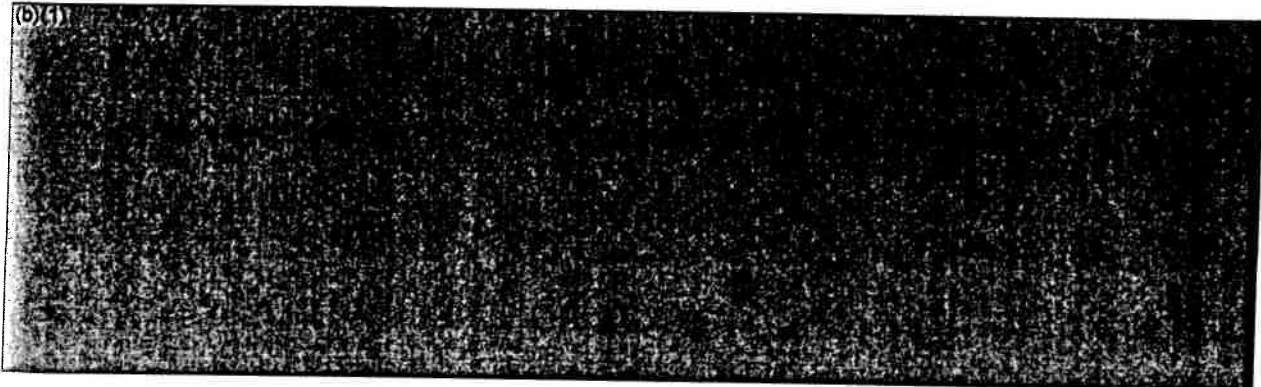
a. (U) Advise the USD(I) and other OSD Principal Staff Assistants on CI activities in cyberspace.

b. (U) Develop, coordinate, and oversee the implementation of CI in cyberspace policy for the USD(I).

c. (U) Represent the USD(I) at DoD and national cyber and CI community forums.

d. (U) Serve as the OSD staff point of contact for all CI in cyberspace issues.

3. (U) DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRECTOR, NSA/CHIEF, CSS). The Director, NSA/Chief, CSS, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 7 of this enclosure, shall:

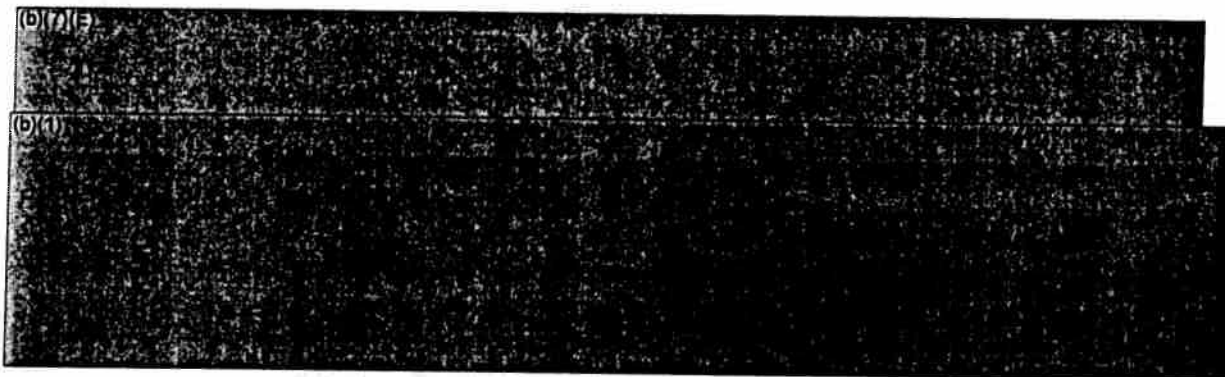


SECRET

DoDI S-5240.23, December 13, 2010

4. (U) DIRECTOR, DCHC. The Director, DCHC, under the authority, direction, and control of the Director, Defense Intelligence Agency, shall:

a. (U) Serve as the DoD CI functional manager for an integrated DoD CI in Cyberspace program.



e. (U) Develop and execute training for Defense CI Components conducting activities in cyberspace in accordance with DoDD 5505.13E (Reference (n)) and DoDI 3305.11 (Reference (o)).

(1) (U) Regularly review DoD CI in cyberspace training courses to ensure relevancy and currency.

(2) (U) Develop training standards and career paths in coordination with the Department of Defense Cyber Crime Center (DC3), the Joint CI Training Academy, Military Departments, and Defense Agencies.

(3) (U) Develop and recommend procedures and standards to certify designated personnel to conduct CI activities in cyberspace in coordination with the USD(I).

f. (U) Conduct CI analysis of cyberspace threats and disseminate products to support CI and enable CI activities in cyberspace.

g. (U) Represent Defense CI Components at national cyber and CI community forums.

h. (U) Recommend CI activities in cyberspace policy to the USD(I).

i. (U) Develop Reference (j) and update, as appropriate.

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

SECRET

DoDI S-5240.23, December 13, 2010

a. (U) Coordinate with Defense CI Components to detect and identify FIE threats to DoD and defense industrial base (DIB) networks pursuant to Reference (b) and in accordance with DoDI 5205.13 (Reference (p)).

b. (U) Oversee DC3 implementation of responsibilities as described in section 11 of this enclosure.

6. (U) HEADS OF DoD COMPONENTS WITH DEFENSE CI COMPONENTS. The Heads of DoD Components with Defense CI components shall:

(b)(7)(E)

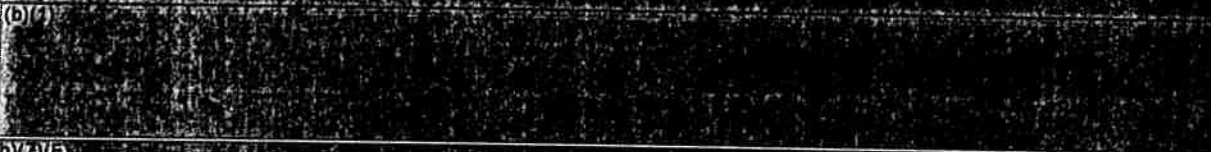


b. (U) Support information operations in accordance with to DoDD 3600.01 (Reference (r)).

(b)(7)(E)



(b)(7)(E)



(b)(7)(E)



(b)(7)(E)



g. (U) Support and participate in DoD CI functional management activities.

h. (U) Ensure that personnel are technically trained and certified to conduct CI activities in cyberspace in accordance with the standards and procedures established by the Director, DCHC, and the Director, DC3.

i. (U) Include threats in cyberspace for all CI awareness, briefing, and reporting programs in accordance with DoDI 5240.6 (Reference (s)). Examples of indicators of potential threat activity on DoD networks are listed in the Table in Enclosure 3 of this Instruction.

7. (U) HEADS OF DoD COMPONENTS WITHOUT DEFENSE CI COMPONENTS. The Heads of DoD Components without Defense CI components shall request CI activities in cyberspace support from their lead CI organization in accordance with DoDI 5240.10 (Reference (t)).

SECRET

DoDI S-5240.23, December 13, 2010

8. (U) COMMANDER, USCYBERCOM. The Commander, USCYBERCOM, under the authority, direction, and control of the Commander, USSTRATCOM, shall:

(b)(1)



(b)(7)(E)



(b)(7)(E)



9. (U) DIRECTOR, DC3. The Director, DC3, under the authority, direction, and control of the ASD(NII)/DoD CIO and in accordance with Reference (n), shall:

a. (U) In coordination with and at the request of the DoD Components, provide complete digital and multimedia (D/MM) forensic services to support CI investigations.

b. (U) Conduct CI-oriented cyber training that:

(1) (U) Provides levels of technical CI cyber training, from basic to advanced, that address FIE cyber tactics, techniques, and procedures to afford CI personnel the requisite technical skills to conduct effective CI activities either in the virtual environment of information systems and computer networks or via exploitation of digital devices in the physical domain in accordance with References (d), (n), and (o).

(2) (U) Supports Reference (j).

(3) (U) Leads the development of computer and web-based cyber training for CI personnel.

c. (U) Serve as the functional lead to develop, evaluate, and test CI techniques used in cyberspace and serve as the central repository of these techniques for Defense CI Components.

SECRET

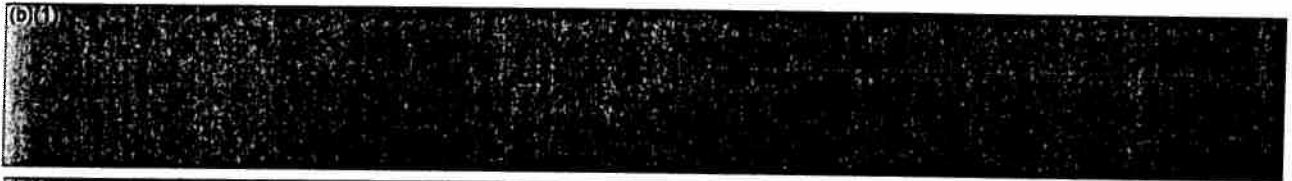
DoDI S-5240.23, December 13, 2010

ENCLOSURE 3

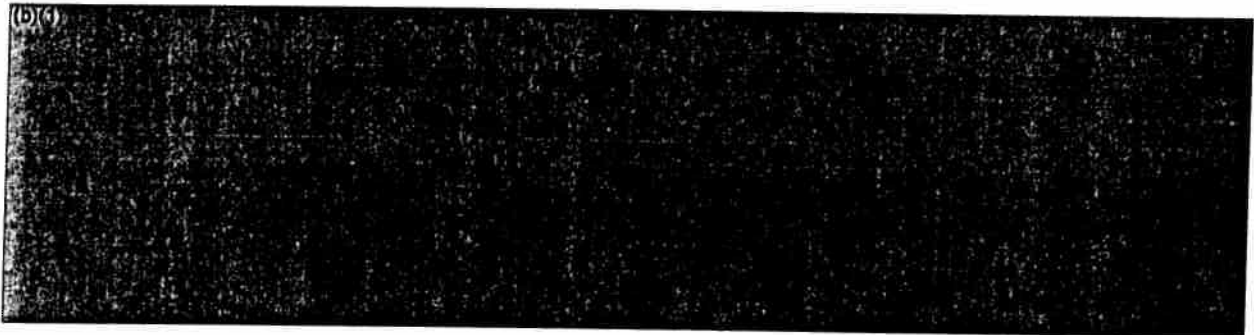
PROCEDURES (U)

1. (U) GENERAL

a. (U) Report all FIE threat information obtained through cyberspace investigative activity, collection, or OFCO as quickly as possible. Perishable information revealing imminent threat shall be reported immediately to the affected installation, command, agency, or component, as well as to the Joint Interagency Task Force-Combating Terrorism, USCYBERCOM, and DCHC.



2. (U) CI SUPPORT TO CYBERSPACE OPERATIONS



b. (U) Support to CND.

(1) (U) DoD CI activities in cyberspace shall be undertaken to deter unauthorized persons from obtaining sensitive or classified information from DoD networks. This includes cyber threat investigations of cyber incidents and intrusions to determine FIE involvement in accordance with Reference (q) and DoDI O-5240.21 (Reference (u)) and proactive efforts to identify foreign intelligence attempts to illegally obtain information that falls within one or more of the DoD CI mission areas.

(2) (U) DoD chief information officers shall work with Defense CI Components to provide sufficient and timely access to networks, network devices, workstations, and digital

SECRET

DoDI S-5240.23, December 13, 2010

information to facilitate inquiries, cyber threat investigations, or other CI activity to determine FIE involvement, except where limited by law. Suspicious activity that is not FIE-related shall be promptly referred to command or law enforcement, as appropriate.

(3) (U) In support of CND and IA, Defense CI Components shall identify emerging and imminent cyber threats and take appropriate actions against FIE threats on DoD, IC, and DIB networks. CI investigative elements shall work with IA and security elements to:

(a) (U) Detect anomalous activity indicative of CI insider threats.

(b) (U) Develop leads for thorough investigative plans.

(c) (U) Conduct analysis, including the appropriate D/MM analysis and analysis of trends and behavioral patterns, to better understand threat plans, intentions, and capabilities.

(d) (U) Recommend appropriate action to protect the integrity of the network or to counter, expose, and/or exploit the FIE threat.

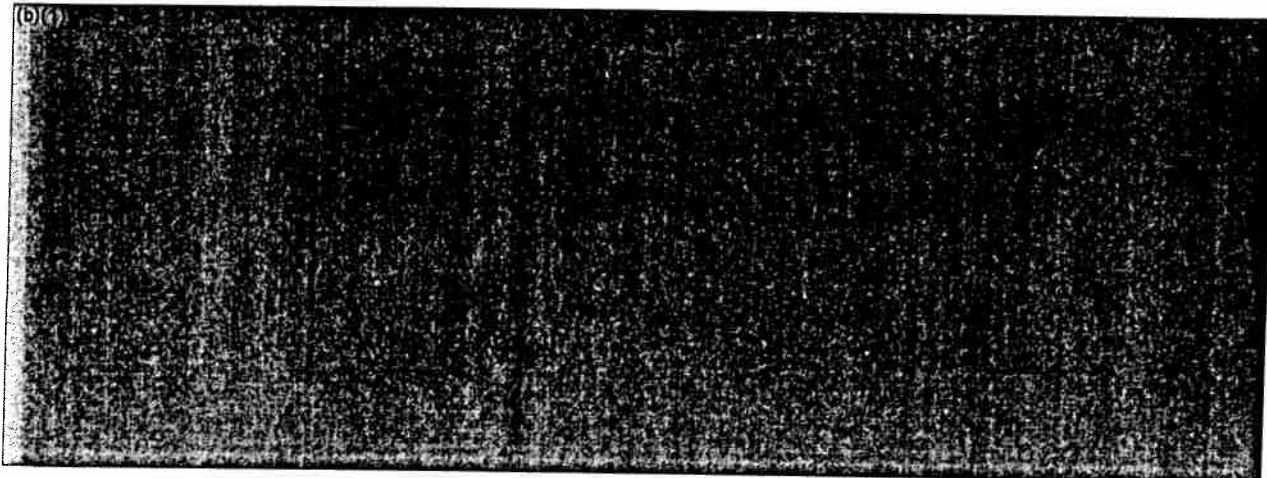
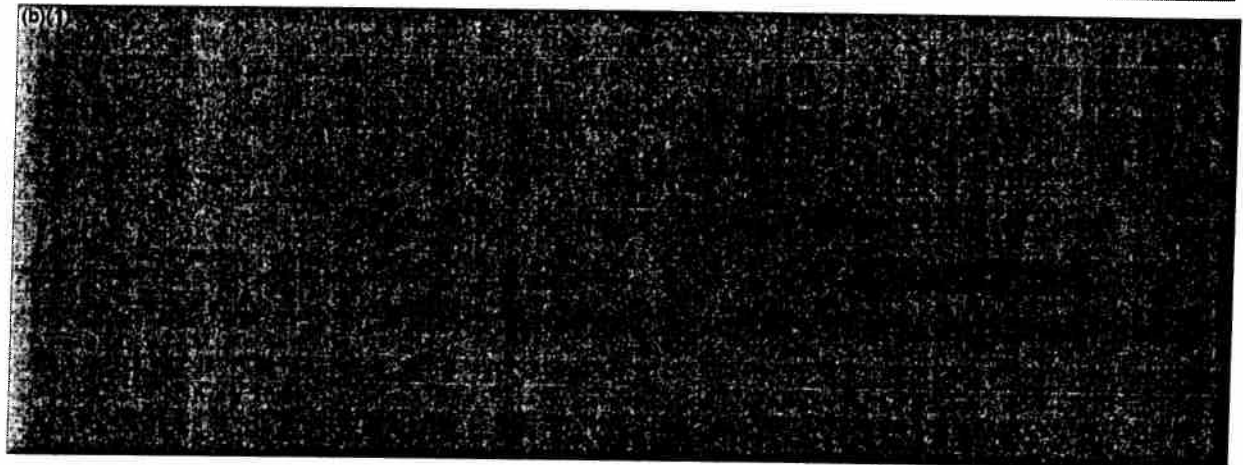
(4) (U) Defense CI Components shall conduct CI activities in cyberspace to identify FIE threats in support of CND. The following table contains examples of indicators related to a CI insider threat or FIE activity on DoD networks that may require further analysis, inquiry, or investigation.

Table. Indicators of Potential Threat Activity on DoD Networks (U)

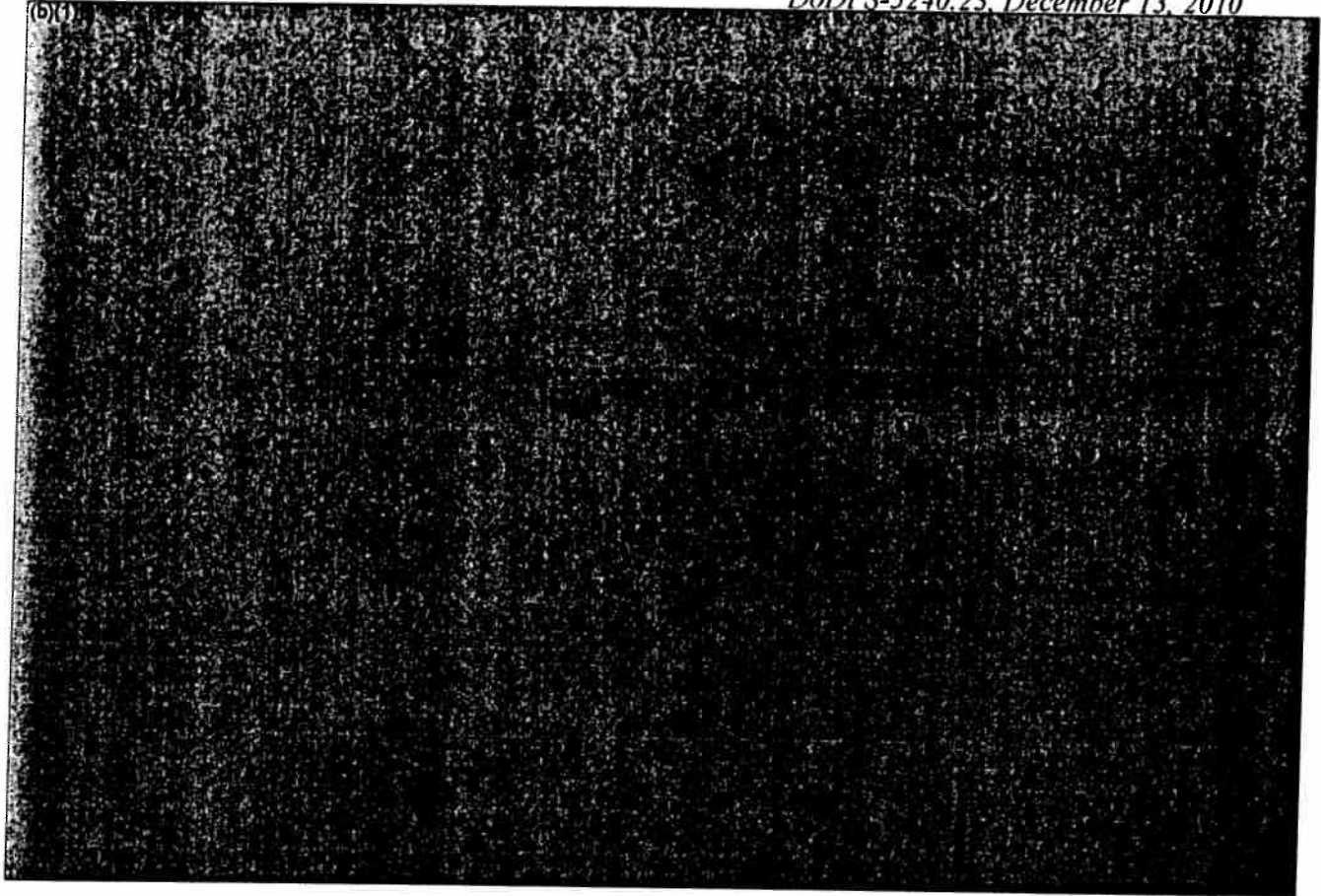
Unauthorized network access.
Suspicious Internet activity, including downloads or uploads of sensitive data.
Indications of unauthorized Universal Serial Bus, removable media, or other transfer devices.
Downloading of non-approved computer applications.
E-mail traffic to foreign destinations.
Data exfiltrated to unauthorized domains.
Excessive and abnormal printing.
Unexplained storage of encrypted data.
Unexplained user accounts.
Hacking or cracking activities.

Table. Indicators of Potential Threat Activity on DoD Networks, Continued (U)

Social engineering, electronic elicitation, e-mail "spoofing," or e-mail "spear-phishing."
Evidence of password cracking, key logging, encryption, or steganography.
Denial of service attacks or suspicious network communications failures.
Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.
Tampering with or introducing unauthorized elements into information systems.
Network spillage incidents or information compromise.
Any credible anomaly, finding, observation, or indicator previously associated with or connected to FIE activity.
Use of DoD account credentials by unauthorized parties.
Any tampering with supply chain.
This table is UNCLASSIFIED.




(b)(1)




(b)(7)(E)



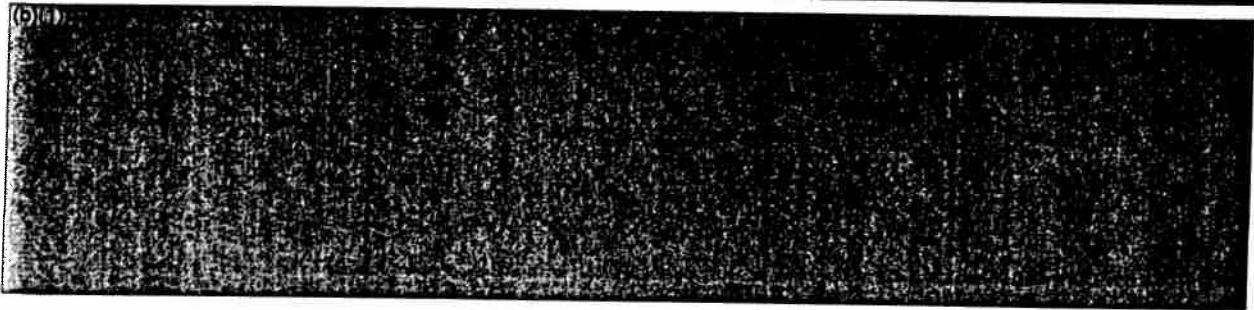
(b)(1)

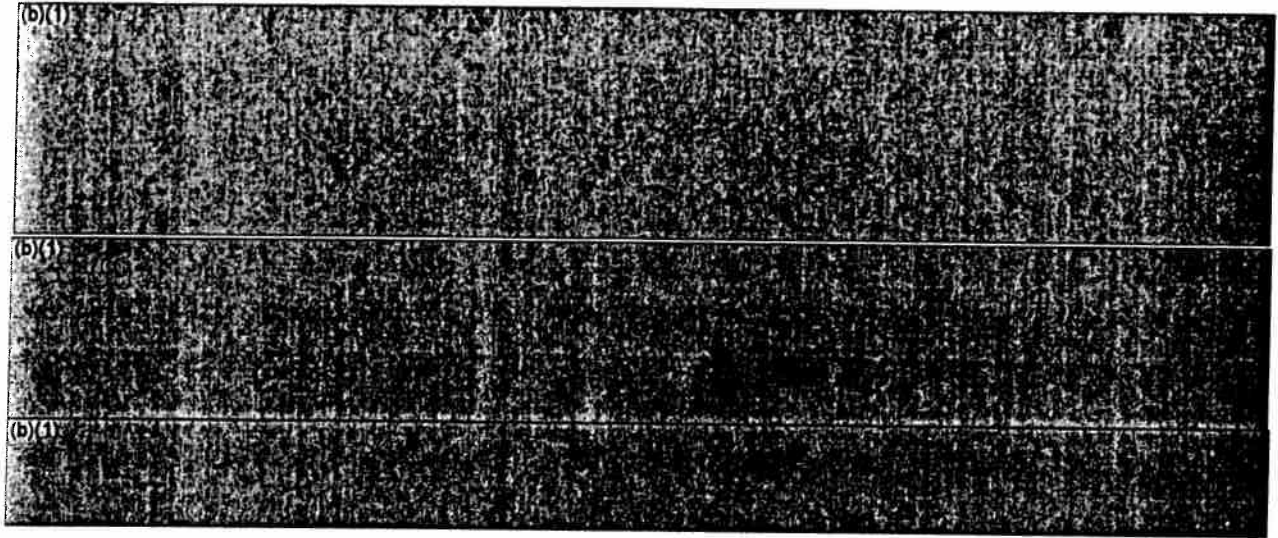


(b)(7)(E)



(b)(1)





GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS (U)

(U) The abbreviations and acronyms in this Glossary are UNCLASSIFIED.

ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
CI	counterintelligence
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
DC3	Department of Defense Cyber Crime Center
DCHC	Defense Counterintelligence and Human Intelligence Center
DIA	Defense Intelligence Agency
DIB	defense industrial base
D/MM	digital and multimedia
DoDD	DoD Directive
DoDI	DoD Instruction
DUSD(HCI&S)	Deputy Under Secretary of Defense for Human Intelligence, Counterintelligence, and Security
FIE	foreign intelligence entity
HUMINT	human intelligence
IA	information assurance
IC	Intelligence Community
IT	information technology
JIPOE	Joint Intelligence Preparation of the Operational Environment
J2X	joint force counterintelligence and human intelligence staff element
NSA/CSS	National Security Agency/Central Security Service
(b)(7)(E)	
(b)(7)(E)	
SIGINT	signals intelligence
USCYBERCOM	United States Cyber Command

USD(I)
USSTRATCOM

Under Secretary of Defense for Intelligence
United States Strategic Command

PART II. DEFINITIONS (U)

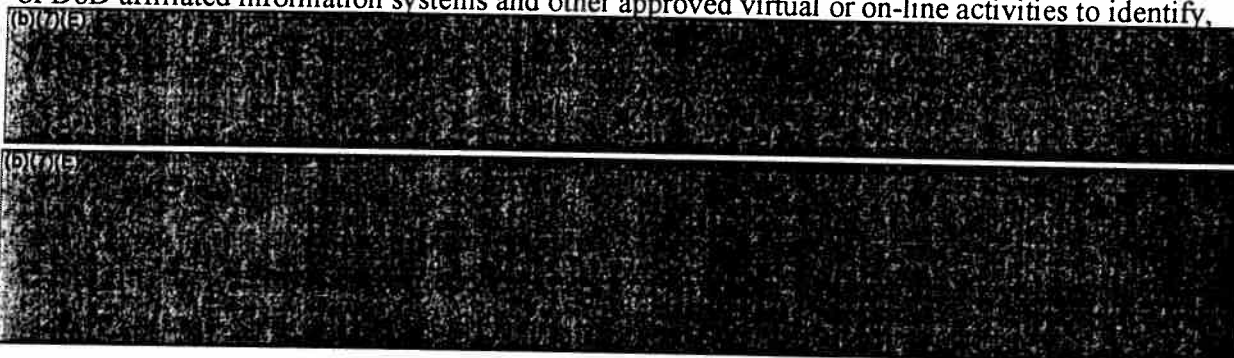
(U) Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

(U) anomalous activity. Network activities that are inconsistent with the expected norms that may suggest FIE exploitation of cyber vulnerabilities or prior knowledge of U.S. national security information, processes, or capabilities.

(U) CI. Defined in Reference (a).

(U) CI activities. Defined in Reference (d).

(U) CI activities in cyberspace. CI activities in cyberspace include those forensics examinations of DoD affiliated information systems and other approved virtual or on-line activities to identify,



(U) CI insider threat. A known or suspected person who uses their authorized access to DoD facilities, systems, equipment, or infrastructure to cause damage, disrupt operations, or commit espionage on behalf of a FIE.

(U) CNE. Defined in Joint Publication 1-02 (Reference (w)).

(U) computer network. The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks.

(U) cyber incident. Defined in Reference (b).



(U) cybersecurity. Defined in Reference (b).

(U) cyberspace. Defined in Reference (w).

(U) cyber threat investigation. Actions taken, consistent with applicable law and Presidential guidance, to determine the identity, location, intent, motivation, capabilities, alliances, funding, or methodologies of one or more FIEs, that has attempted to penetrate or has, in fact, penetrated a DoD, IC, or DIB information system

(U) Defense CI Component. Defined in Reference (c).

(U) digital tradecraft. The conduct, topics, or techniques of modern espionage or CI that employ digital or cyber means.

(U) FIE. Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, blocks or impairs U.S. intelligence collection, influences U.S. policy, or disrupts U.S. systems and programs. This term includes a foreign intelligence and security service and international terrorists.

(U) information system. Defined in Reference (w).

(U) intrusion. Unauthorized access to a DoD, DIB, or critical infrastructure network, information system, or application.

(b)(7)(E)

(b)(1)

(b)(7)(E)