Department of Defense
INSTRUCTION

SUBJECT: Cybersecurity Activities Support to DoD Information Network Operations

References: See Enclosure 1

1. <u>PURPOSE</u>. In accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (a)), this instruction:

    a. Reissues DoDD O-8530.1 (Reference (b)) as a DoD Instruction (DoDI) and incorporates and cancels DoDI O-8530.2 (Reference (c)) to establish policy and assign responsibilities to protect the Department of Defense information network (~~DoDIN~~*DODIN*) against unauthorized activity, vulnerabilities, or threats.

    b. Supports the Joint Information Environment (JIE) concepts as outlined in JIE Operations Concept of Operations (CONOPS) (Reference (d)).

    c. Supports the formation of Cyber Mission Forces (CMF), development of the Cyber Force Concept of Operations and Employment, evolution of cyber command and control, cyberspace operations doctrine in Joint Publication 3-12 (Reference (e)), and evolving cyber threats.

    d. Supports the Risk Management Framework (RMF) requirements to monitor security controls continuously, determine the security impact of changes to the ~~DoDIN~~*DODIN* and operational environment, and conduct remediation actions as described in DoDI 8510.01 (Reference (f).

    e. Cancels Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum (Reference (g)).

2. <u>APPLICABILITY</u>. This instruction:

    a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) 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 DoD (referred to collectively in this instruction as the "DoD Components").

b. The United States Coast Guard (USCG). The USCG will adhere to DoD cybersecurity requirements, standards, and policies in this instruction 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 (cn)).

~~b~~c. Applies to the ~~DoDIN~~*DODIN*. The ~~DoDIN~~*DODIN* includes DoD information technology (IT) (e.g., DoD-owned or DoD-controlled information systems (ISs), platform information technology (PIT) systems, IT products and services) as defined in DoDI 8500.01 (Reference (h)) and control systems and industrial control systems (ICSs) as defined in National Institute (NIST) Special Publication (SP) 800-82 (Reference (i)) that are owned or operated by or on behalf of
DoD Components.

~~c~~d. Applies to commercial cloud computing services that are subject to the DoD Cloud Computing Security Requirements Guide (Reference (j)), developed by Director, Defense Information Systems Agency (DISA).

~~d~~e. Applies to cleared defense contractors who operate pursuant to DoD 5220.22-M (Reference (k)) and the National Industrial Security Program (NISP) in accordance with DoDI 5220.22 (Reference (l)), to the extent that its requirements are made applicable through incorporation into contracts.

~~e~~f. Applies to mission partner systems connected to the ~~DoDIN~~*DODIN* in accordance with, and to the extent set forth in, a contract, memorandum of agreement (MOA), support agreement, or international agreement, subject to and consistent with DoDI 4000.19 (Reference (m) and DoDD 5530.03 (Reference (n)).

~~f~~g. Does not alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartmented information (SCI) as directed by Executive Order 12333 (Reference (o)) and other laws and regulations.

3. <u>POLICY</u>. It is DoD policy that:

a. DoD protects (i.e., secures and defends) the ~~DoDIN~~*DODIN* and DoD information using key security principles, such as isolation; containment; redundancy; layers of defense; least privilege; situational awareness; and physical or logical segmentation of networks, services, and applications to allow mission owners and operators, from the tactical to the DoD level, to have confidence in the confidentiality, integrity, and availability of the ~~DoDIN~~*DODIN* and DoD information to make decisions.

b. DoD integrates technical and non-technical capabilities to implement DoD information network operations (~~DoDIN~~*DODIN* operations) and defensive cyberspace operations (DCO) internal defensive measures directed by global, regional, and DoD Component authorities to protect the ~~DoDIN~~*DODIN* consistent with References (e), (f), and (h) ~~and DoDI 8410.02 (Reference (p))~~.

c. DoD integrates and employs a number of cybersecurity activities to support ~~DoDIN~~*DODIN* operations and DCO internal defensive measures in response to vulnerabilities and threats as described in Reference (e). These activities include:

(1) Vulnerability assessment and analysis.

(2) Vulnerability management.

(3) Malware protection.

(4) Continuous monitoring.

(5) Cyber incident handling.

(6) ~~DoDIN~~*DODIN* user activity monitoring (UAM) for the DoD Insider Threat Program.

(7) Warning intelligence and attack sensing and warning (AS&W).

d. DoD IT will be aligned to DoD network operations and security centers (NOSCs). The NOSC and supporting cybersecurity service provider(s) will provide any required cybersecurity services to aligned systems.

e. DoD designated cybersecurity service providers will be authorized to provide cybersecurity services in accordance with DoD O-8530.~~0~~*0*1-M (Reference (~~q~~*p*)). When cybersecurity services are provided, both the cybersecurity service provider and the system owner security responsibilities will be clearly documented.

f. DoD will help protect the ~~DoDIN~~*DODIN* through criminal or counterintelligence investigations or operations in support of ~~DoDIN~~*DODIN* operations.

g. Compliance with directed cyberspace operations will be a component of individual and unit accountability.

h. Contracts, MOAs, support agreements, international agreements, or other applicable agreements or arrangements governing the interconnection of the ~~DoDIN~~*DODIN* and mission partners' systems developed in accordance with References (m) and (n) must identify:

(1) Specific ~~DoDIN~~*DODIN* operations responsibilities of DoD and mission partners;

(2) The cybersecurity requirements for the connected mission partners' systems;

(3) The protection requirements for DoD data resident on mission partner systems; and

(4) Points of contact for mandatory reporting of security incidents.

i. Data on the cybersecurity status of the ~~DoDIN~~*DODIN* and connected mission partner systems will be shared across the DoD enterprise in accordance with Reference (h), DoDI 8410.03 (Reference (~~r~~*q*)), and DoDI 8320.02 (Reference (~~s~~*r*)) to maintain ~~DoDIN~~*DODIN* situational awareness. DoD will:

　　(1) Use automated capabilities and processes to display ~~DoDIN~~*DODIN* operations and cybersecurity data, and ensure that the required data effectively satisfies the mission objectives.

　　(2) Ensure ~~DoDIN~~*DODIN* operations and cybersecurity data are visible, accessible, and understandable, trusted, and interoperable both vertically between superior and subordinate organizations and horizontally across peer organizations and mission partners in accordance with Reference (~~s~~*r*).

4. RELEASABILITY. **Cleared for public release**. This instruction is available on ~~the Internet from~~ the DoD Issuances Website at ~~http://www.dtic.mil/whs/directives~~ *http://www.esd.whs.mil/DD/*.

5. EFFECTIVE DATE. This instruction is effective March 7, 2016.

Terry A. Halvorsen
DoD Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. DoD Component Activities to Protect the ~~DoDIN~~*DODIN*
4. Cybersecurity Integration Into ~~DoDIN~~*DODIN* Operations
Glossary

TABLE OF CONTENTS

FIGURES

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014
(b) DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001 (hereby cancelled)
(c) DoD Instruction O-8530.2, "Support to Computer Network Defense (CND)," March 9, 2001 (hereby cancelled)
(d) Joint Information Environment Operations Sponsor Group, "Joint Information Environment Operations Concept of Operations (JIE Operations CONOPS)," Version 2.0, September 18 2014[1]
(e) Joint Publication 3-12, "Cyberspace Operations," February 5, 2013
(f) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014*, as amended*
(g) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, "Guidance for Computer Network Defense Response Actions," February 26, 2003 (hereby cancelled)
(h) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(i) National Institute of Standards and Technology (NIST) Special Publication 800-82, Revision 2, "Guide to Industrial Control Systems (ICS) Security," May 2015[2]
(j) Defense of Defense Security Requirements Guide, "Department of Defense (DoD) Cloud Computing Security Requirements Guide, "Version 1, Release ~~13~~, ~~January 12, 2015~~ *March 6, 2017*[3]
(k) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended
(l) DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011
(m) DoD Instruction 4000.19, "Support Agreements," April 25, 2013
(n) DoD Directive 5530.3, "International Agreements," June 11, 1987, as amended
(o) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
~~(p)   DoD Instruction 8410.02, "NetOps for the Global Information Grid (GIG)," December 19, 2008~~
(~~q~~*p*) DoD O-8530.1-M, "Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program," December 17, 2003
(~~r~~*q*) DoD Instruction 8410.03, "Network Management (NM)," August 29, 2012
(~~s~~*r*) DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013
(~~t~~*s*) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise *(DoD IE)*" ~~February 10, 2009~~ *March 17, 2016*

---

[1] JIE CONOPS Version 2.0 can be found on Intelink at: https://dodcioext.osd.mil/SitePages/Initiative_JIE.aspx
[2] NIST Special Publications are available at: http://csrc.nist.gov/publications/PubsSPs.html.
[3] Cloud Computing Security Requirements Guide is available at:
http://iase.disa.mil/cloud_security/Documents/Forms/Allitems.aspx

(~~u~~*t*) DoD Chief Information Officer, "The DoD Architectural Framework (DoDAF) Specifications, Version 2.02," August 2010[4]

(~~v~~*u*) DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," July 25, 2006

(~~w~~*v*) DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including and National Security Systems (NSS)," May 21, 2014

(~~x~~*w*) Committee on National Security Systems Policy No. 29, "National Secret Enclave Connection Policy," May 2013

(~~y~~*x*) DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014*, as amended*

(~~z~~*y*) Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21, 2012

(~~aa~~*z*) Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011

(~~ab~~*aa*) Committee on National Security Systems Directive (CNSSD) No. 504, "Directive on Protecting National Security Systems from Insider Threat," February 4, 2014[5]

(~~ac~~*ab*) Chairman of the Joint Chiefs of Staff Execute Order (EXORD), "Modification (MOD) to EXORD To Implement Cyberspace Operations Command and Control (C2)," 141627ZNovember 2014[6]

(~~ad~~*ac*) DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, as amended

(~~ae~~*ad*) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999

(~~af~~*ae*) Section 932 of Public Law 113-66, "Authorities, Capabilities, and Oversight of the United States Cyber Command," December 26, 2013

(~~ag~~*af*) Deputy Secretary of Defense Memorandum, "Guidance Regarding Cyberspace Roles, Responsibilities, Functions, and Governance within the Department of Defense," June 9, 2014

(~~ah~~*ag*) Secretary of Defense Memorandum, "Designation of the DoD Principal Cyber Advisor," July 17, 2014

(~~ai~~*ah*) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," October 24, 2014, as amended

(~~aj~~*ai*) Section 142 of Title 10, United States Code

(~~ak~~*aj*) DoD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010

(~~al~~*ak*) DoD Instruction O-3115.07, "Signals Intelligence (SIGINT)," September 15, 2008, as amended

(~~am~~*al*) Chairman of the Joint Chiefs of Staff Manual 6510.03, "Department of Defense Cyber Red Team Certification and Accreditation," February 28, 2013

(~~an~~*am*) DoD Directive 5105.21, "Defense Intelligence Agency (DIA)," March 18, 2008

(~~ao~~*an*) DoD Directive 5105.42, "Defense Security Service (DSS)," August 3, 2010, as amended

---

[4] DoDAF is available at: http://dodcio.defense.gov/Library/DoDArchitectureFramework .aspx

[5] CNSSD No. 504 can be found on Secret Internet Protocol Router Network (SIPRNET) at:
http://www.iad.nsa.smil.mil/resources/library/cnss_section/pdf/CNSSD_504.pdf

[6] CJCS EXORD can be found on Intelink at:
https://intelshare.intelink.sgov.gov/sites/jointstaff/j3/ddgo/cod/Cyber%20C2%20Documents/Forms/Allitems.aspx

(~~ap~~*ao*) DoD Manual 5220.22, Volume 3, "National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control or Influence (FOCI), April 17, 2014

(~~aq~~*ap*) DoD Directive 5141.02, "Director of Operational Test and Evaluation (DOT&E)," February 2, 2009

(~~ar~~*aq*) DoD Instruction 5010.41, "Joint Test and Evaluation (JT&E) Program," September 12, 2005

(~~as~~*ar*) DoD Directive 5145.01, "General Counsel of the Department of Defense (GC DoD)," December 2, 2013, as amended

(~~at~~*as*) DoD Instruction 5025.01, "DoD Issuances Program," ~~June 6, 2014~~ *August 1, 2016*, as amended

(~~au~~*at*) DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012, as amended

(~~av~~*au*) Chairman of the Joint Chiefs of Staff Notice 3500.01, "2015-2018 Chairman's Joint Training Guidance," October 30, 2014

(~~aw~~*av*) Deputy Under Secretary of Defense for Acquisition, Technology and Logistics Memorandum, "Real-Property-related Industrial Control System Cybersecurity," March 19, 2014

(~~ax~~*aw*) Subchapter III of Chapter 35 of Title 44, United States Code (also known as the "Federal Information Security Modernization Act (FISMA) of 2014")

(~~ay~~*ax*) Appendix III to Office of Management and Budget Circular No. A-130, "Security of Federal Automated Information Resources," November 28, 2000, as amended

(~~az~~*ay*) DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014*, as amended*

(~~ba~~*az*) Chairman of the Joint Chiefs of Staff Manual 3122.01A, "Joint Operation Planning and Execution System (JOPES) Volume I, Planning Policies and Procedures," September 29, 2006[7]

(~~bb~~*ba*) Chairman of the Joint Chiefs of Staff Manual 3122.02D, "Joint Operation Planning and Execution System (JOPES) Volume III, Timed Phased Force and Deployment Data Development and Deployment Execution," March 17, 2011, as amended

(~~bc~~*bb*) Joint Publication 3-35, "Deployment and Redeployment Operations," January 31, 2013

(~~bd~~*bc*) DoD Directive 3000.06, "Combat Support Agencies (CSAs)," June 27, 2013*, as amended*

(~~be~~*bd*) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

(~~bf~~*be*) DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012

(~~bg~~*bf*) DoD Regulation 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

(~~bh~~*bg*) DISA Circular 300-110-3, "Defense Information System Network (DISN) Security Classification Guide (U)," September 27, 2012[8]

---

[7] CJCS Manuals 3122.01A and 3122.02D are available on Intelink at CJCS/JS Directives Electronic Library (SIPRNET) at:
http://intelshare.intelink.sgov.gov/sites/jointstaff/SJS/IMD/Directives/Shared%20Documents/Forms/CJCS%20Manuals.aspx.

[8] DISA Publications and Issuances (CAC Required):
https://disa.deps.mil/ext/resource/disa_publications_issuances/default.aspx

(~~bi~~*bh*) Joint Worldwide Intelligence Communications Systems (JWICS) Security Classification Guide (SCG)," current version[9]

(~~bj~~*bi*)DoD Instruction O-3600.02, "Information Operations (IO) Security Classification Guidance," November 28, 2005

(~~bk~~*bj*) DoD Directive 5100.03, "Support of the Headquarters of Combatant and Subordinate Unified Commands," February 9, 2011

(~~bl~~*bk*) DoD Instruction 3020.41, "Operational Contract Support (OCS)," December 20, 2011*, as amended*

(~~bm~~*bl*) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015*, as amended*

(~~bn~~*bm*) Unified Command Plan, April 6, 2011, as amended[10]

(~~bo~~*bn*) Secretary of Defense Memorandum, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," June 23, 2009

(~~bp~~*bo*) Commander, United States Strategic Command (CDRUSSTRATCOM) OPORD "OPERATION GLADIATOR PHOENIX (U)," February 11, 2011[11]

(~~bq~~*bp*) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011

(~~br~~*bq*) National Institute of Standards and Technology Special Publication 800-115, "Technical Guide to Information Security Testing and Assessment," September 2008

(~~bs~~*br*) Chairman of the Joint Chiefs of Staff Manual 6510.02, "Information Assurance Vulnerability Management (IAVM) Program," November 5, 2013[12]

(~~bt~~*bs*) National Institute of Standards and Technology Special Publication 800-40, Revision 3, "Guide to Enterprise Patch Management Technologies," July 2013

(~~bu~~*bt*) National Institute of Standards and Technology Special Publication 800-83, Revision 1, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops," July 2013

(~~bv~~*bu*) National Institute of Standards and Technology Special Publication 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," September 2011

(~~bw~~*bv*) National Institute of Standards and Technology Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010*, as amended*

(~~bx~~*bw*) National Institute of Standards and Technology Special Publication 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011[6]

(~~by~~*bx*) Chairman of the Joint Chiefs of Staff Manual 6510.01B, "Cyber Incident Handling Program," July10, 2012

---

[9] Classification guide can be found on JWICS at: http://jwics.ic.gov/Security/Documents/JWICS_SCG%20docx.pdf
[10] Available on to authorized users at: https://intellipedia.intelink.sgov.gov/wiki/Unified_Command_Plan/
[11] Available at:
https://www.cybercom.smil.mil/J3/orders/OPORD11_002/STRATCOM%20OPORD%20Op%20Gladiator%20Phoenix.pdf
[12] CJCS Manual is available on Intelink at CJCS/JS Directives Electronic Library (SIPRNET) at:
http://intelshare.intelink.sgov.gov/sites/jointstaff/SJS/IMD/Directives/Shared%20Documents/Forms/CJCS%20Manuals.aspx

(~~bz~~*by*) Committee on National Security Systems Instruction No. 1010, "~~24x7 Computer Incident Response Capability (CIRC) on National Security Systems~~*Cyber Incident Response*," ~~October 3, 2012~~ *December 16, 2016*

(~~ca~~*bz*) National Institute of Standards and Technology Special Publication 800-61, Revision 2, "Computer Security Incident Handling Guide," August 2012[6]

(~~cb~~*ca*) DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended

(~~cc~~*cb*) Committee on National Security Systems Policy No. 18, "National Policy on Classified Information Spillage," June 2006[6]

(~~cd~~*cc*) Committee on National Security Systems Instruction No. 1001, "National Instruction on Classified Information Spillage," February 2008[6]

(~~ee~~*cd*) DoD Instruction 5240.26, "Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat," May 4, 2012, as amended

(~~cf~~*ce*) Joint Publication 2-0, "Joint Intelligence," October 22, 2013

(~~cg~~*cf*) DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015

(~~ch~~*cg*) Defense Information Systems Agency, "Defense Information Systems Network (DISN) Connection Process Guide (CPG)," current version

(~~ci~~*ch*) DoD 5220.22-R, "Industrial Security Regulation," December 4, 1985

(~~cj~~*ci*) Subpart 4.4 of the Federal Acquisition Regulation

(~~ck~~*cj*) DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012

(~~cl~~*ck*) Defense Federal Acquisition Regulation Supplement 252.204-7012, "Safeguarding of Unclassified Controlled Technical Information," current edition

(~~cm~~*cl*) Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015[13]

(~~cn~~*cm*) ~~Joint Publication 1-02,~~ *Office of the Chairman of the Joint Chiefs of Staff,* "~~Department of Defense~~ *DoD* Dictionary of Military and Associated Terms," current edition

(cn) 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[14]

---

[13]Available through the Internet at http://www.cnss.gov

[14]*Available through the Internet 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. <u>DoD CHIEF INFORMATION OFFICER (DoD CIO)</u>. In accordance with Reference (a), the DoD CIO:

    a. Establishes DoD policy and provides guidance and oversight for integrating cybersecurity activities to support ~~DoDIN~~*DODIN* operations and DCO internal defensive measures and to strengthen accountability through the cyberspace operations chain of command to protect the ~~DoDIN~~*DODIN* in coordination with the Under Secretary of Defense for Policy (USD(P)), the Principal Cyber Advisor (PCA), the Under Secretary of Defense for Intelligence (USD(I)), the CJCS, the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), and the Commander, U. S. Strategic Command (CDRUSSTRATCOM).

    b. Provides strategic management, guidance, and direction to DoD Component efforts to plan, program, budget, develop, and implement the capability to protect the ~~DoDIN~~*DODIN* in coordination with the USD(P) based on the DoD Enterprise Architecture in accordance with DoDD 8000.01 (Reference (~~t~~*s*)) and the evolving JIE architecture.

    c. Ensures capabilities are developed and incorporated into the DoD Architectural Framework (Reference (~~u~~*t*)) in accordance with ~~DoDD 5105.19 (Reference (v~~*u*~~)) and~~ DoDI 8330.01 (Reference (~~w~~*v*)) to protect the ~~DoDIN~~*DODIN*.

    d. Oversees the development and implementation of DoD cybersecurity architectures and capabilities to protect the ~~DoDIN~~*DODIN*, in coordination with CDRUSSTRATCOM.

    e. Oversees the DoD Component cybersecurity service provider authorization process and DoD Component compliance with criteria established in Reference (~~q~~*p*)

    f. Validates in coordination with Director, DISA, cybersecurity standards established by Federal mission partner organizations connected to the ~~DoDIN~~*DODIN* comply with equivalent cybersecurity requirements and to those standards described in Committee on National Security Systems Policy (CNSSP) No. 26 Reference (~~x~~*w*).

    g. Oversees process and approves requests for the interconnection of mission partners' systems to the ~~DoDIN~~*DODIN* through a point-to-point connection or a demilitarized zone (DMZ).

        (1) Approves the authorized interconnection points to the ~~DoDIN~~*DODIN* for either a mission partner DMZ interconnection (e.g., Federal (FED) DMZ or Releasable (REL) DMZ) or a point-to-point interconnection.

(2) In coordination with DISA, maintains a list of validated non-DoD Federal mission partner organizations that meet the equivalency requirements required of DoD cybersecurity service providers.

(3) Provides to mission partners DoD's requirements for risk tolerance for interconnecting mission partners' systems and the ~~DoDIN~~*DODIN*.

(4) Ensures that the roles and responsibilities for managing and mission partner interconnection to the ~~DoDIN~~*DODIN*, including cybersecurity requirements, are documented in a contract, MOA, support agreement, or international agreement document. These agreements must be in accordance with References (m) and (n).

h. Coordinates with the USD(I) and the Director, Defense Security Service (DSS), on cybersecurity requirements for the NISP.

i. Coordinates with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and CDRUSSTRATCOM on:

(1) Needs and requirements for DoD-wide research and technology investments and activities to protect the ~~DoDIN~~*DODIN*.

(2) Development of and, where applicable, the acquisition of automated capabilities for ~~DoDIN~~*DODIN* situational awareness that support ~~DoDIN~~*DODIN* operations and DCO internal defensive measures. Capabilities will be consistent with the approved Joint Capabilities Integration and Development System (JCIDS) document.

j. Participates or designates representation on national and Federal Chief Information Officer (CIO) cybersecurity related coordination groups, as required.

k. Develops policy and strategy, including auditing and UAM standards. Helps the USD(P), the USD(I), and the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) develop guidelines and procedures for implementation of standards for the DoD Insider Threat Program in accordance with DoDD 5205.16 (Reference (~~y~~*x*)), and contained in Presidential Memorandum (Reference (~~z~~*y*)), Executive Order 13587 (Reference (~~aa~~*z*)), and Committee on National Security Systems Directive (CNSSD) No. 504 (Reference (~~ab~~*aa*))reference.

l. Develops metrics that will measure the cybersecurity status of the ~~DoDIN~~*DODIN* leveraging existing standards and guidelines for audit and assessment processes in coordination with CDRUSSTRATCOM.

m. Reviews the cybersecurity posture of systems authorized to operate outside the ~~DoDIN~~*DODIN*. Such systems will be reviewed, before granting a ~~DoDIN~~*DODIN* waiver to operate outside the ~~DoDIN~~*DODIN*, to ensure that there is an appropriate level of cybersecurity to protect personnel, information, and equipment within the system operating boundary.

n. Participates or designates representation on Federal and DoD cybersecurity-related panels and boards, as required.

2. <u>DIRECTOR, DISA</u>. Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in section 14 of this enclosure, the Director, DISA:

a. Protects DoD transport and enterprise services in accordance with *DoDI 5105.19 (*Reference (~~v~~*u*)*)* in coordination with CDRUSSTRATCOM, joint, and DoD Component NOSCs.

b. Plans for, mitigates, and executes ~~DoDIN~~*DODIN* operations and DCO internal defensive measures at the DoD global and DoD enterprise level, as directed by CDRUSSTRATCOM.

c. Serves as the Commander, Joint Forces Headquarters- ~~DoDIN~~*DODIN* (JFHQ-~~DoDIN~~*DODIN*), a subordinate headquarters under the Commander, U~~nited.~~ S*tates.* Cyber Command (CDRUSCYBERCOM) in accordance with CJCS Execute Order (EXORD) (Reference (~~ac~~*ab*)) that establishes the framework for global ~~DoDIN~~*DODIN* operations.

d. Provides ~~DoDIN~~*DODIN* situational awareness of DISA operated DoD transport and enterprise services, including enterprise network data and analytics for supported DoD Components to measure the impact of changes in the ~~DoDIN~~*DODIN*, such as cybersecurity, availability,
and compliance.

e. Provides and maintains a cybersecurity and network defense plan for DoD enterprise transport and enterprise services critical nodes.

f. Supports CDRUSSTRATCOM compliance and operational readiness inspections of the ~~DoDIN~~*DODIN*.

g. Develops, maintains, and implements the general service (GENSER) DoD cybersecurity service provider processes in accordance with Reference (~~q~~*p*) and in coordination with the DoD CIO, the CDRUSSTRATCOM, and the Director, Defense Intelligence Agency (DIA).

(1) Maintains the GENSER maturity evaluation criteria found in Reference (~~q~~*p*) in coordination with the DoD Component cybersecurity service providers, the CDRUSSTRATCOM, and the DoD CIO.

(2) Functions as the evaluator for GENSER DoD cybersecurity services in accordance with Reference (~~q~~*p*).

(3) Conducts evaluation of DoD Component cybersecurity service providers' services as directed by CDRUSSTRATCOM. Evaluation documents with a recommendation are provided to the CDRUSSTRATCOM to authorize the service provider to offer cybersecurity services for GENSER systems.

(4) Provides cybersecurity services on a subscription basis to any DoD Component organization, Federal department, or Federal agency that does not establish or otherwise subscribe to a DoD GENSER cybersecurity service provider.

(5) Provides cybersecurity guides and best practices guidelines for use by DoD and mission partners in coordination with the CDRUSSTRATCOM; the Director, DIA; DIRNSA/CHCSS; and the DoD CIO.

(6) Verifies DoD cybersecurity service provider qualifications in accordance with DoD 8570.01-M (Reference (~~ad~~*ac*)) during evaluations or inspections.

(7) Validates Federal mission partner's capability to provide cybersecurity services and capabilities that are equivalent to those specified in Reference (~~q~~*p*) in coordination with DoD CIO.

(a) Maintains a list of validated mission partner organizations with equivalent cybersecurity services and capabilities aligned with mission partner systems connected to the ~~DoDIN~~*DODIN*.

(b) Provides cybersecurity services and capabilities to mission partners connected to the ~~DoDIN~~*DODIN* through a DMZ, such as FED DMZ or REL DMZ, on a subscription basis when requested.

h. Serves as a technical advisor to the DoD CIO for DoD-wide capability requirements to protect the ~~DoDIN~~*DODIN* in coordination with the Director, DIA, DIRNSA/CHCSS, and the CDRUSSTRATCOM.

3. <u>USD(AT&L)</u>. The USD(AT&L) provides oversight of the development and acquisition of capabilities that protect the ~~DoDIN~~*DODIN*. Oversees the development and, where applicable, the acquisition of automated capabilities for ~~DoDIN~~*DODIN* situational awareness that support ~~DoDIN~~*DODIN* operations and DCO internal defensive measures, in coordination with the DoD CIO, DIRNSA/CHCSS, and the CDRUSSTRATCOM. Capabilities will be consistent with the approved JCIDS initial capabilities documents.

4. <u>ASSISTANT SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (ASD(R&E))</u>. Under the authority, direction, and control of the USD(AT&L), the ASD(R&E) oversees all DoD-wide research and technology investments and activities to:

a. Protect the ~~DoDIN~~*DODIN*.

b. Provide developments and results to the Assistant Secretary of Defense for Acquisition in support of their acquisition oversight responsibilities.

5. <u>USD(P)</u>. Consistent with the responsibilities assigned in DoDD 5111.1 (Reference (~~ae~~*ad*)) on the formulation of national security and defense policy, the USD(P):

 a. Supervises cyber activities related to offensive missions, defense of the United States, and defense of the ~~DoDIN~~*DODIN*, including oversight of policy and operational considerations, resources, personnel, acquisition (in consultation with the USD(AT&L)), technology (in consultation with the USD(AT&L) and DoD CIO), and on military cyber forces and activities in accordance with section 932 of Public Law 113-66 (Reference (~~af~~*ae*)) and Deputy Secretary of Defense Memorandum (Reference (~~ag~~*af*)).

 b. Coordinates with the USD(AT&L), USD(I), and DoD CIO on the development of DoD cyberspace operations policy, including ~~DoDIN~~*DODIN* operations and DCO internal defensive measures policy to protect the ~~DoDIN~~*DODIN*.

6. <u>ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY</u>. Under the authority, direction, and control of USD(P), and as the PCA designated by Secretary of Defense Memorandum (Reference (~~ah~~*ag*)), will in coordination with relevant Principal Staff Advisors, serve as the principle advisor to the Secretary of Defense on cyberspace operations and missions and advise the Secretary with respect to matters pertaining to those identified in Reference (~~ag~~*af*).

7. <u>USD(I)</u>. Consistent with the responsibilities assigned in DoDD 5143.01 (Reference (~~ai~~*ah*)), the USD(I):

 a. Ensures that Defense intelligence, counterintelligence, and security programs support DoD's requirements to protect the ~~DoDIN~~*DODIN*;

 b. Oversees the use of National Intelligence Program and Military Intelligence Program resources to support DoD's efforts to protect the ~~DoDIN~~*DODIN*. Ensures the equitable and appropriate use of those resources across the Defense Intelligence Enterprise;

 c. Oversees DoD intelligence activities, including warning intelligence and AS&W support to ~~DoDIN~~*DODIN* operations and DCO internal defensive measures;

 d. Coordinates with DoD CIO to develop UAM guidelines and procedures to implement the requirements specified in References (~~y~~*x*), (~~z~~*y*), and (~~aa~~*z*);

 e. Provides security advice and support to the DoD CIO and separately to the USD(AT&L) when acquisition programs utilizing cleared defense contractors are involved; and

 f. Oversees policy and management of the NISP and develops and approves Reference (l).

8. <u>DIRNSA/CHCSS</u>. Under the authority, direction, and control of the USD(I), consistent with section 142 of Title 10, United States Code (Reference (~~aj~~*ai*) in addition to the cybersecurity-related responsibilities in DoDD 5100.20 (Reference (~~ak~~*aj*)) and the responsibilities in section 14 of this enclosure, the DIRNSA/CHCSS:

   a. Conducts DoD-wide capability research and technology development to protect the ~~DoDIN~~*DODIN*.

      (1) Provides support for capability research to the CDRUSSTRATCOM, the DoD CIO cybersecurity architect, and the USD(AT&L).

      (2) Conducts and manages basic research, applied research, advanced technology development, and technology component development and prototyping in order to advance the state-of-the-art for capabilities used to protect the ~~DoDIN~~*DODIN* and conduct ~~DoDIN~~*DODIN* operations and DCO internal defensive measures.

      (3) Develops proofs-of-concept, prototype systems, and system pilots to enable more effective capabilities to protect the ~~DoDIN~~*DODIN*.

      (4) Advises and assists in the design of standards and interfaces to integrate existing capabilities.

      (5) Maintains a comprehensive view of all capabilities gaps, shortfalls, and research, development, and technology transfer requirements across the DoD.

   b. Provides and coordinates technical and analytical support to DoD Components, as requested by the CDRUSSTRATCOM.

   c. Provides the CDRUSSTRATCOM, joint, and the DoD Component NOSCs and their supporting cybersecurity service providers with warning intelligence and AS&W information in accordance with Reference (~~ak~~*aj*) and DoDI O-3115.07 (Reference (~~al~~*ak*)). In support of DoD organizations, provides:

      (1) Detection, alerting, and response capabilities to mitigate threats to the ~~DoDIN~~*DODIN*.

      (2) Warning intelligence information through reporting or posting on secure websites.

      (3) Overall DoD-wide long-term effectiveness trend and pattern analysis to support the protection of the ~~DoDIN~~*DODIN* as informed by situational awareness of ~~DoDIN~~*DODIN* operations and DCO internal defensive measures and the results of DoD assessments, evaluations, inspections, and exercises.

      (4) Monitoring and analysis of vulnerabilities and adversary threat to the ~~DoDIN~~*DODIN*.

(5) Multi-source reporting on threats to the ~~DoDIN~~*DODIN*.

(6) Technology, information, expertise, and other support to the DoD NOSCs and their supporting cybersecurity service providers, as required.

d. Supports the DoD CIO cybersecurity architect and the DoD Components in the development of capabilities to protect the ~~DoDIN~~*DODIN*, within the DoD Enterprise and the JIE architectures.

e. Evaluates DoD Cyber Red Teams in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.03 (Reference (~~am~~*al*)) and CDRUSSTRATCOM direction.

f. Provides evaluation documents with authorization recommendations to the CDRUSSTRATCOM for these teams to conduct operations across ~~DoDIN~~*DODIN* outside of their DoD Component's authorization boundaries (e.g., DoD-owned or -operated systems).

g. Serves as the technical advisor to the DoD CIO on DoD-wide capability requirements to protect the ~~DoDIN~~*DODIN* in coordination with the Director, DISA.

9. <u>DIRECTOR, DIA</u>. Under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 14 of this enclosure and consistent with the responsibilities in DoDD 5105.21 (Reference (~~an~~*am*)), the Director, DIA:

a. Develops, maintains, and implements the DoD special enclave (SE) cybersecurity service provider processes in accordance with Reference (~~q~~*p*) and in coordination with the DoD CIO; the CDRUSSTRATCOM and the Director, DISA.

(1) Maintains the SE maturity evaluation criteria found in Reference (~~q~~*p*) in coordination with the DoD Components with SE cybersecurity providers, CDRUSSTRATCOM, and the DoD CIO.

(2) Functions as the evaluator of SE DoD cybersecurity services in accordance with Reference (~~q~~*p*).

(3) Conducts evaluation of DoD Component cybersecurity service providers' services as directed by the CDRUSSTRATCOM. Evaluation documents with a recommendation are provided to the Director, DIA designated office to authorize the cybersecurity service provider to offer SE cybersecurity services.

(4) Provides cybersecurity services on a subscription basis to any DoD Component organization that does not establish or otherwise subscribe to a DoD SE cybersecurity service provider.

(5) Verifies DoD SE cybersecurity service providers' qualifications in accordance with Reference (~~ad~~*ac*) during evaluations or inspections.

(6) Establishes advisory and alert procedures for SE DoD Components and their supporting cybersecurity service providers.

b. Coordinates with the Intelligence Community Chief Information Officer and DIRNSA/CHCSS on the design, development, and maintenance of capabilities to protect DoD and intelligence community (IC) SEs operated by DoD Components (e.g., Joint Worldwide Intelligence Communications System (JWICS)).

c. Coordinates the incorporation of IC information network situational awareness information into the ~~DoDIN~~*DODIN* situational awareness capabilities and processes in coordination with DIRNSA/CHCSS; and provides DoD SE network situational awareness information to the intelligence community.

d. Provides DoD-wide threat analysis focused on the ~~DoDIN~~*DODIN* in support of the United States Strategic Command (USSTRATCOM) and the other DoD Components in coordination with DIRNSA/CHCSS.

e. Provides for the collection, processing, and dissemination of all-source, finished intelligence to identify potential threats, provide indications of threat activity, and disseminate warnings of threat activities against the ~~DoDIN~~*DODIN* and IC networks.

f. Provides all source analysis of adversary threats and finished intelligence in support of ~~DoDIN~~*DODIN* situational awareness for the CDRUSSTRATCOM, joint and DoD Component NOSCs, and their supporting cybersecurity service providers.

10. <u>DIRECTOR, DSS</u>. Under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 14 of this enclosure, and consistent with the responsibilities assigned in DoDD 5105.42 (Reference (~~ao~~*an*)), the Director, DSS:

a. Oversees the NISP, including cleared defense contractor systems processing classified information.

b. Requires companies operating under a foreign ownership, control, or influence mitigation agreement to develop and maintain an Electronic Communications Plan as described in Volume 3 of DoD Manual (DoDM) 5220.22 (Reference (~~ap~~*ao*)).

c. Provides ~~DoDIN~~*DODIN* situational awareness and threat alerts to cleared defense contractors on threats to their systems.

d. Disseminates information to identify potential threats, provide indications of threat activity, and disseminate warnings of threat activities against cleared defense contractor systems.

11. <u>DIRECTOR, OPERATIONAL TEST AND EVALUATION (DOT&E)</u>. The DOT&E:

a. Oversees the conduct of operational test and evaluation of ~~DoDIN~~*DODIN* operations and DCO internal defensive measures to assess joint interoperability and evaluate joint technical and operational concepts to protect the ~~DoDIN~~*DODIN* and future JIE consistent with the responsibilities assigned in DoDD 5141.02 (Reference (~~aq~~*ap*)) and DoDI 5010.41 (Reference (~~ar~~*aq*)).

b. Oversees the conduct of cybersecurity assessments during major exercises consistent with Reference (~~aq~~*ap*).

12. <u>GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE (GC DoD)</u>. The GC DoD provides legal advice regarding legal issues related to ~~DoDIN~~*DODIN* operations and DCO internal defensive measures, with the exception of those undertaken by the IG DoD in accordance with DoDD 5145.01 (Reference (~~as~~*ar*)).

13. <u>IG DoD</u>. The IG DoD:

a. Develops policy guidance, as appropriate, for law enforcement and criminal investigations that relate to cyberspace in accordance with DoDI 5025.01 (Reference (~~at~~*as*)) and DoDD 5106.01 (Reference (~~au~~*at*)).

b. Through the Director, Defense Criminal Investigation Service, and in accordance with Reference (~~au~~*at*), provides data to cyber incident ~~DoDIN~~*DODIN* situational awareness databases, as the IG DoD deems appropriate.

14. <u>DoD COMPONENT HEADS</u>. The DoD Components heads:

a. Conduct ~~DoDIN~~*DODIN* operations and DCO defensive internal measures in accordance with CDRUSSTRATCOM and DoD Component orders and directives to protect their respective portion of the ~~DoDIN~~*DODIN*.

b. Implement actions to ensure ~~DoDIN~~*DODIN* readiness, respond to potential adversary operations, or disrupt potential adversary presence in the ~~DoDIN~~*DODIN*. Examples of actions include: verifying accounts having administrative privileges, reestablishing known good software baselines on servers, ensuring use of common access cards and resetting passwords.

c. Practice and evaluate ~~DoDIN~~*DODIN* operations and DCO internal defensive measures during exercises (e.g., joint or continuity of operations exercises) to ensure that processes and procedures can be evaluated and the effectiveness of pre-planned actions or potential directed DCO internal measures in a denied or contested cyber environment can be measured against opposing forces (OPFOR) operations and other CMF team requirements as described in CJCS Notice 3500.01 (Reference (~~av~~*au*)). This includes testing and evaluating DoD Component ICSs

to ensure survivability and to preclude a mission disabling event occurring in a cyber contested environment as described in Deputy USD(AT&L) memorandum (Reference *(awav*)).

d. Use organic or external cybersecurity activities and capabilities to protect DoD Component owned or operated portion of the ~~DoDIN~~*DODIN* in accordance with References (f) and (h); subchapter III of chapter 35 of Title 44, U. S. Code, also known as the "Federal Information Security Modernization Act (FISMA) of 2014" (Reference (~~ax~~*aw*)); Appendix III to Office of Management and Budget Circular A-130 (Reference (~~ay~~*ax*)); and federal and DoD issuances applicable to these activities.

e. Ensure DoD Component systems are aligned to a joint or DoD Component NOSC to receive and comply with orders or directives from USSTRATCOM and their DoD Component.

f. Oversee the implementation of all directed actions required by USSTRATCOM or its Component for their respective owned or operated portion of the ~~DoDIN~~*DODIN*.

(1) Implement directed actions in accordance with CDRUSSTRATCOM orders or other directives issued through the CDRUSCYBERCOM or subordinate Commander, JFHQ-~~DoDIN~~*DODIN* in accordance with Reference (~~ac~~*ab*). Examples of an order or directive include an operation order (OPORD), fragmentary order, tasking order (TASKORD), EXORD, vulnerability management alert, and vulnerability management bulletin. The collection of information must be approved and licensed in accordance with the procedures in Volume 1 of DoDM 8910.01 (Reference (~~az~~*ay*)).

(2) Coordinate with USSTRATCOM or other affected DoD Components actions or measures that could affect the ~~DoDIN~~*DODIN* outside their Component.

g. Plan for, coordinate, request, and support deployment of USSTRATCOM CMF.

(1) Force deployments in support of joint operations will be in accordance with CJCSM 3122.01A (Reference (~~ba~~*az*)), CJCSM 3122.02D (Reference (~~bb~~*ba*)), Joint Publication (JP) 3-35 (Reference (~~bc~~*bb*)), and DoDD 3000.06 (Reference (~~bd~~*bc*)).

(2) Provide CMF teams support in accordance with the deployment order.

(3) Notify DoD counterintelligence and law enforcement agencies responsible for the affected portion of the ~~DoDIN~~*DODIN* of CMF deployment, and any counterintelligence or law enforcement support requested.

(4) Provide cyber mission forces required access to DoD Component owned or operated portions of the ~~DoDIN~~*DODIN* to support of DoD cyberspace operations in accordance with Secretary of Defense and CDRUSSTRATCOM orders and other directives.

h. Establish a DoD Component-wide sensor grid and ~~DoDIN~~*DODIN* situational awareness capability to share data on cybersecurity activities and to collaborate with other organizations in coordination with the CDRUSSTRATCOM; the Director, DISA; DIRNSA/CHCSS; and with

review of the Cyber Investment Management Board (CIMB) to support ~~DoDIN~~*DODIN* operations and DCO internal defensive measures.

i. Designate DoD Component-owned or -operated portions of the ~~DoDIN~~*DODIN* as either SE or GENSER.

j. Validate that cybersecurity services provided to DoD Component organizations or offered by a DoD Component cybersecurity provider to external organizations have been evaluated in accordance with Reference (~~q~~*p*) and that CDRUSSTRATCOM has authorized the service provider to provide those cybersecurity services.

k. Provide information to the DoD CIO, as requested, to support the ~~DoDIN~~*DODIN* architectures, the cybersecurity service provider process, and capability development activities to protect the ~~DoDIN~~*DODIN*.

l. Develop intelligence requirements (IRs) to facilitate timely decision making for the protection of the DoD Component-owned or -operated portion of the ~~DoDIN~~*DODIN*. Submit those IRs to supporting intelligence organizations.

m. Validate requests by DoD Component organizations to be designated as a DoD cyber red team authorized to conduct operations across the ~~DoDIN~~*DODIN* in accordance with Reference (~~am~~*al*), and prioritize requests, if required.

n. Inform the IG DoD when cybersecurity deficiencies in the ~~DoDIN~~*DODIN* contribute to a security breach or failure and are the result of noncompliance with DoD standards or contractual provisions.

o. Ensure that all users understand and follow the policy and guidance to protect classified and controlled unclassified information and prevent unauthorized disclosures on DoD IT.

    (1) Classified Information

        (a) Unauthorized disclosure or data spillage involving classified information will be identified as a negligent discharge of classified information incident to be reported and investigated in accordance with Volume 3 of DoDM 5200.01 (Reference (~~be~~*bd*)). The investigation must determine whether the incident was willful, negligent, or inadvertent.

        (b) Classified information may be processed only on systems approved for such use, at the required level of classification and access control, in accordance with Reference (~~be~~*bd*).

    (2) Controlled Unclassified Information (CUI)

        (a) Unauthorized disclosures of CUI will be handled and reported in accordance with Volume 4 of DoDM 5200.01(Reference (~~bf~~*be*)) or guidance for specific types of CUI provided by the DoD Component Head or information owner (e.g., DoD 5400.11-R (Reference (~~bg~~*bf*)) for privacy information).

(b) If possible, electronic transmission CUI and privacy information (e.g., data, website, or e-mail) will be approved by secure communications systems or systems utilizing other protective measures such as encryption to protect confidentiality and integrity of CUI and privacy information to avoid unauthorized disclosure.

p. Ensure personnel creating and compiling vulnerability and technical details on the configuration of systems are aware of the need to refer to applicable security classification guides, such as DISA Circular 300-110-3 (Reference (~~bh~~*bg*)), JWICS Security Classification Guide (Reference (~~bi~~*bh*)), and DoDI O-3600.02 (Reference (~~bj~~*bi*)), for guidance on classifying and marking information.

(1) Vulnerability information specific to DoD IT systems, and technical details on the configuration of DoD IT systems, will be handled, at a minimum, as controlled unclassified information or at classification level of the systems in accordance with applicable classification guidance such as References (~~bh~~*bg*), (~~bi~~*bh*), and (~~bj~~*bi*).

(2) CDRUSSTRATCOM will provide amplifying classification guidance in directives and orders for specific threat, vulnerability, or configuration information, and directed ~~DoDIN~~*DODIN* operations or DCO internal measures.

q. Ensure all personnel understand cybersecurity best practices and compliance requirements and procedures, as appropriate.

(1) Establish criteria for inclusion of cybersecurity compliance with individual and unit readiness, assessments, and evaluations.

(2) Employ sanctions against individuals or units in accordance with the severity of non-compliance with cybersecurity policies, directives, and orders.

r. Ensure all ~~DoDIN~~*DODIN* acquisitions plan for and integrate cybersecurity requirements into system life-cycles.

s. Ensures that the requirements of this DoDI are incorporated, as appropriate, into contracts, MOAs, international agreements, and other agreements with non-DoD mission partners.

15. <u>SECRETARIES OF THE MILITARY DEPARTMENTS</u>. In addition to the responsibilities in section 14 of this enclosure, the Secretaries of the Military Departments:

a. Ensure that their respective Departments' law enforcement and counterintelligence communities share cyberspace incident-related investigative, counterintelligence, and operational information with the CDRUSSTRATCOM and with Director, DSS, for cleared defense contractors, as authorized. Military Department law enforcement and counterintelligence communities will coordinate with CDRUSSTRATCOM and Director, DSS, as appropriate,

regarding investigation versus protection cost-benefit decisions to minimize negative impacts to investigations and operations.

b. Develop Military Department-specific requirements to support the provision of protection capabilities within the Military Department portion of the ~~DoDIN~~*DODIN*, including Service use of Federal- or DoD-mandated enterprise capabilities.

c. Provide cybersecurity services to Combatant Commands and other organizations in accordance with support agreements. Support to Combatant Commands will be in accordance with DoDD 5100.03 (Reference (~~bk~~*bj*)) and DoDI 3020.41 (Reference (~~bl~~*bk*)).

16. <u>CJCS</u>. In addition to the responsibilities in section 14 of this enclosure, the CJCS:

a. Oversees the development of doctrine, instructions, manuals, and capability documents to facilitate the integration of ~~DoDIN~~*DODIN* operations, DCO internal defensive measures and supporting cybersecurity activities and capabilities into joint operations.

b. Advises on and assesses joint military requirements for capabilities to protect the ~~DoDIN~~*DODIN* assisted by the Joint Requirements Oversight Council in accordance with DoDI 5000.02 (Reference (~~bm~~*bl*)).

c. Provides advice, guidance, direction, and assistance for capability interoperability and supportability matters for the protection of the ~~DoDIN~~*DODIN* in accordance with Reference (~~w~~*v*) and in coordination with DoD Components.

d. Ensures that exercise OPFOR conducting cyberspace operations are as realistic as possible for the ~~DoDIN~~*DODIN* with limited constraints on the exercise OPFOR for reasons of safety or operational security. Additional OPFOR capabilities requirements will be reviewed in coordination with the CIMB to identify overall costs and to minimize the potential for duplication of effort.

e. Reviews professional military education curricula to ensure inclusion of relevant topics related to ~~DoDIN~~*DODIN* operations, DCO internal defensive measures, and the supporting activities and capabilities to protect the ~~DoDIN~~*DODIN*, in coordination with the USD(P).

17. <u>CDRUSSTRATCOM</u>. In addition to the responsibilities in section 14 of this enclosure, the CDRUSSTRATCOM:

a. Synchronizes planning for cyberspace operations in accordance with the Unified Command Plan (Reference (~~bn~~*bm*)).

b. Directs the security, operations, and defense of the ~~DoDIN~~*DODIN* through the CDRUSCYBERCOM in accordance with References (~~bn~~*bm*), the Secretary of Defense Memorandum (Reference (~~bo~~*bn*)), and OPORD OPERATION GLADIATOR PHOENIX

(Reference (~~bp~~*bo*)). CDRUSSTRATCOM is vested with directive authority for cyberspace operations (DACO), delegable to CDRUSCYBERCOM to issue orders and directives to all DoD Components for the execution of Global ~~DoDIN~~*DODIN* operations and DCO internal defensive measures to compel unity of action to secure, operate and defend the ~~DoDIN~~*DODIN* in accordance with Reference (~~ac~~*ab*).

c. Executes assigned responsibilities to protect the ~~DoDIN~~*DODIN* in accordance with Reference (~~bn~~*bm*) and CJCS Instruction 6510.01F (Reference (~~bp~~*bo*)).

d. Advocates for the capability requirements of the DoD Components to protect the ~~DoDIN~~*DODIN*.

e. Plans for, coordinates, and deploys cyber mission forces to protect the ~~DoDIN~~*DODIN* in accordance with References (~~ba~~*az*), (~~bb~~*ba*), (~~bc~~*bb*), (~~bd~~*bc*), and deployment orders.

f. Plans for, directs, and deconflicts DCO internal defensive measures to search actively for unauthorized activity and advanced persistent threats within the ~~DoDIN~~*DODIN* in accordance with Reference (~~bp~~*bo*) and in coordination with DIRNSA/CHCSS; Director, DIA; Director, DISA; and other DoD Components.

g. Establishes, maintains, and directs standardized tactics, techniques, and procedures in which commanders and DoD Component heads ensure network availability, the security and defense of mission critical or essential systems, and that integrates approved response options to protect warfighter, business, and intelligence functions in cyberspace.

h. Provides the DoD CIO; Director, DIA; DIRNSA/CHCSS; and the CJCS, for the purposes of including their consideration as components of readiness assessments, with:

(1) Summaries of findings from ~~DoDIN~~*DODIN* vulnerability assessments, intrusion assessments, evaluations, inspections, exercises, DoD cyber red team operations, and lessons learned from military operations.

(2) Associated findings addressing systemic issues, disclosures of sensitive network architecture information, exploited vulnerabilities, successful tactics and techniques, and trends in poor user security practices.

i. Supports the development of cyberspace IRs and provides support to the Combatant Commands.

j. Establishes requirements and direction for situational awareness for ~~DoDIN~~*DODIN* operations and DCO internal defensive measures including actionable warning intelligence and AS&W information on adversary threats.

k. Oversees and directs actions by NOSCs and supporting GENSER and SE cybersecurity service providers in coordination with the DoD Components.

l. Supports the cybersecurity service provider process in accordance with Reference (~~q~~*p*).

(1) Continuously monitors the performance of GENSER and SE cybersecurity service providers and their plans of action and milestones (POA&Ms) from evaluations or inspections to ensure compliance with requirements in accordance with Reference (~~q~~*p*).

(2) Authorizes DoD cybersecurity service providers to offer GENSER cybersecurity services to DoD Components or DoD mission partners following DISA evaluation.

(3) Reviews reciprocity requests and supporting GENSER or SE evaluation documentation for joint CDRUSSTRATCOM and Director, DIA authorization for a cybersecurity service provider to provide both GENSER and SE cybersecurity services, as required, in coordination with the Director, DISA; and the Director, DIA.

m. Authorizes DoD cyber red teams to conduct operations across the ~~DoDIN~~*DODIN*, following DIRNSA/CHCSS evaluation.

n. Provides procedures for the reporting of DoD cyber red team, blue team, inspection team, or CMF team operational network activities conducted as part of an operation, evaluation, vulnerability assessment, intrusion assessment, or inspection to the DoD CIO, CJCS, and the other DoD Component heads.

o. Establishes operational requirements for shared information from an enterprise sensor grid for ~~DoDIN~~*DODIN* situational awareness automated capability in coordination with the CJCS and the DoD CIO.

p. Coordinates with the USD(AT&L) and DoD CIO on the development and, where applicable, the acquisition of automated capabilities for ~~DoDIN~~*DODIN* situational awareness that support DoD information network operations and protection of the ~~DoDIN~~*DODIN*.

q. Verifies that operational requirements are included in the development of the ~~DoDIN~~*DODIN* operations portions of the DoD Enterprise and the JIE architectures.

r. Maintains awareness of and deconflicts ~~DoDIN~~*DODIN* operations and DCO internal defensive measures including ongoing or projected assessments, intrusion assessments, evaluations, inspections, red team operations, exercises, and operations directed in the ~~DoDIN~~*DODIN* in coordination with the DoD Components.

s. Develops joint standardized inspection criteria for cybersecurity activities supporting ~~DoDIN~~*DODIN* operations and DCO internal defensive measures.

t. Conducts joint compliance inspections of DoD Component cybersecurity activities in accordance with Reference (bp)-assigned cyberspace operations responsibilities.

ENCLOSURE 3

DoD COMPONENT ACTIVITIES TO PROTECT THE ~~DoDIN~~*DODIN*

1. GENERAL

a. This enclosure identifies a set of cybersecurity activities that are required for ~~DoDIN~~*DODIN* operations and DCO internal defensive measures to protect the ~~DoDIN~~*DODIN*.

b. These activities include, but are not limited to:

(1) Vulnerability Assessment and Analysis.

(2) Vulnerability Management.

(3) Malware Protection.

(4) Information Security Continuous Monitoring (ISCM).

(5) Cyber Incident Handling.

(6) ~~DoDIN~~*DODIN* UAM for DoD Insider Threat Program.

(7) Warning Intelligence.

c. These activities enable DoD Components to implement active or passive actions and measures to mitigate or counter vulnerabilities and threats to the ~~DoDIN~~*DODIN*. By effectively uniting the skills and capabilities of assigned cybersecurity personnel, supporting service providers and CMF will enable DoD to protect the ~~DoDIN~~*DODIN*.

2. VULNERABILITY ASSESSMENT AND ANALYSIS ACTIVITIES. Vulnerability assessment and analysis are vital proactive activities to determine the adequacy of cybersecurity measures for ~~DoDIN~~*DODIN* assets. Vulnerability assessment and analysis apply a variety of techniques (e.g., network discovery, network and host vulnerability scanning, penetration testing) to identify vulnerabilities and to assess whether ~~DoDIN~~*DODIN* assets conform to recommended security policies and configurations. The DoD Vulnerability Assessment and Analysis activities:

a. Provide the capability to determine systematically the current adequacy of cybersecurity measures for the DoD Component portion of the ~~DoDIN~~*DODIN*; identify deficiencies; provide data from which to predict the effectiveness of proposed cybersecurity measures; and confirm the adequacy of such measures after implementation. Guidance on information security testing and assessment can be found in NIST SP 800-115 (Reference (~~br~~*bq*)).

b. Employ organic and external capabilities to conduct vulnerability assessments, intrusion assessments, insider threat assessments, penetration testing, cyber red team operation assessments, or inspections to evaluate the ability of or compliance with DoD Component organization defense plans, ~~DoDIN~~*DODIN* operations' activities, and cybersecurity service provider ability to provide required supporting cybersecurity services.

c. Perform network and host vulnerability scanning to verify vulnerability remediation, identify open ports, vulnerable software, and misconfigured services on a network, and identifies specific host operating system and application misconfigurations and vulnerabilities in accordance with Reference (~~bq~~*bp*) and CJCSM 6510.02 (Reference (~~bs~~*br*)).

d. Provide the CDRUSSTRATCOM visibility and insight into the cybersecurity status of their respective portion of the ~~DoDIN~~*DODIN* to assess risk to the ~~DoDIN~~*DODIN* through reports, findings, and analyses resulting from vulnerability assessments, intrusion assessments, evaluations, inspections, exercises, DoD Cyber Red Team operations, or lessons learned from military operations.

e. Validate that DoD Component cyber red teams employed externally to the DoD Component's portion of the ~~DoDIN~~*DODIN* are authorized to conduct those operations in accordance with Reference (~~am~~*al*).

f. Inform the CDRUSSTRATCOM and the DIRNSA/CHCSS of ongoing DoD Component cyber red team operations. If a DoD Component has multiple authorized cyber red teams, a single office or organization must be designated as the point of contact for maintaining visibility of all the DoD Component cyber red team operations and coordinating activities with USSTRATCOM and the DIRNSA/CHCSS.

3. <u>VULNERABILITY MANAGEMENT PROGRAM</u>. Vulnerability management requires preemptive actions by DoD organizations to identify and prevent the exploitation of ~~DoDIN~~*DODIN* vulnerabilities. Vulnerability management is used by DoD organization to identify, categorize, remediate, and mitigate vulnerabilities in ~~DoDIN~~*DODIN* assets. The primary objective of vulnerability management is to detect and remediate vulnerabilities in a pre-emptive approach based on threat and mission operations. Vulnerabilities will either be mitigated or accepted based on risk management (e.g., threat impact is low; correction would affect mission operations). The DoD Vulnerability Management Program:

a. Requires a system inventory including hardware equipment, operating systems, and software applications and applies DoD required and organization-accepted standard security configurations to improve the effectiveness and reduce the time and resources required to conduct ~~DoDIN~~*DODIN* operations and DoD Component or CDRUSSTRATCOM DCO internal defensive measures.

b. Provides the capability to receive threat, vulnerability, and attack notifications; and take directed corrective actions to mitigate potential vulnerabilities or threats to the DoD

Component's portion of the ~~DoDIN~~*DODIN* in accordance with Reference (~~bs~~*br*), and as described in NIST SP 800-40, Revision 3 (Reference (~~bt~~*bs*)).

c. Establishes a vulnerability management process and procedures that provide positive control to implement actions on the DoD Component-owned or operated portion of the ~~DoDIN~~*DODIN* in accordance with CDRUSSTRATCOM orders or other directives issued through the CDRUSCYBERCOM, such as a TASKORD or vulnerability management alert for patching or configuration changes.

d. Verifies DoD Component organizations and individuals take directed actions, maintain POA&Ms and provide compliance status through the relevant DoD Component reporting chain to CDRUSCYBERCOM in accordance with Reference (~~bs~~*br*) and DoD Component head and CDRUSCYBERCOM guidance.

4. <u>MALWARE PROTECTION PROCESS</u>. Malware protection that is properly implemented and maintained helps prevent damaging attack by countering unauthorized changes made to software and hardware by malicious code that could otherwise leak information or disable capabilities. Malware protection helps an organization protect against and respond to software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of a system. The DoD malware protection process:

a. Provides the capability to prevent malware incidents such as from malicious code, malicious logic, or malicious applets; detects and analyzes malware; contains the spread of malware and prevents further damage; eradicates the malware from infected hosts; employs mitigating actions to prevent reinfection; and restores functionality and removes temporary containment measures as described in NIST SP 800-83, Revision 1 (Reference (~~bu~~*bt*)).

b. Employs malware detection mechanisms at ~~DoDIN~~*DODIN* entry and exit points (e.g., firewalls, email servers, Web servers, proxy servers, remote access servers) and at endpoint devices (e.g., workstations, servers, mobile computing devices) on the network to detect and remove malicious code transported by electronic mail, electronic mail attachments, Web accesses, removable media or other means, or inserted through the exploitation of ~~DoDIN~~*DODIN* vulnerabilities.

c. Configures malware detection mechanisms to perform periodic scans of the ~~DoDIN~~*DODIN* in accordance with current DoD and DoD Component guidance.

d. Incorporates malware incident prevention and handling into awareness training.

5. <u>ISCM</u>. ISCM provides constant observation and analysis of the operational states of systems to provide decision support regarding situational awareness and deviations from expectations. Overall ISCM furnishes ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, cyber hygiene, and cybersecurity operational readiness. The DoD ISCM:

a. Establishes the capability to capture, correlate, analyze, and provide continuous visibility into DoD assets; and the security status of DoD Components represented by the security domains monitored; assesses the compliance, effectiveness, and changed state of security controls protecting the DoD Component-owned or -operated portion of the ~~DoDIN~~*DODIN*; and maintains ongoing awareness of information security, threats, and vulnerabilities to support organizational risk management decisions. Guidance on ISCM can be found in NIST SP 800-137 (Reference (~~bv~~*bu*)), NIST SP 800-37 (Reference (~~bw~~*bv*)), and NIST SP 800-39 (Reference (~~bx~~*bw*)).

b. Supports ~~DoDIN~~*DODIN* operations by providing ongoing awareness of threats and security status of traffic, fault, performance, bandwidth, route, and associated network management areas. ISCM also supports monitoring of employee use of the ~~DoDIN~~*DODIN* to detect anomalous activity in accordance with Reference (~~y~~*x*).

c. Supports ~~DoDIN~~*DODIN* operations and DCO internal defensive measures by providing ongoing awareness and security status of reportable cyber events and incidents. This capability supports timely informed and actionable cyber incident handling decisions in accordance with CJCSM 6510.01B (Reference (~~by~~*bx*)).

d. Supports the RMF by providing ongoing awareness and security status of the posture of an organization's information and systems. This capability supports timely informed and actionable risk decisions and continued RMF decisions in accordance with Reference (f).

e. Synchronizes requirements through the DoD Information Security Continuous Monitoring Working Group (ISCMWG). The DoD ISCMWG is the assigned governance body for ISCM collaboration, cooperation, and coordination; the principal venue by which DoD synchronizes policy, strategy, and requirements for ISCM implementation across DoD national security systems (NSSs) and non-NSSs.

6. <u>CYBER INCIDENT HANDLING PROGRAM</u>. DoD cyber incident handling program protects, monitors, analyzes, and detects unauthorized or anomalous activity on the ~~DoDIN~~*DODIN*. Information such as classified data spills, unauthorized access, and outages are collected and distributed through a joint incident management system. The DoD Cyber Incident Handling Program:

a. Provides the capability to analyze and respond to events or cyber incidents to mitigate any adverse operational or technical impact on the DoD Component-owned or -operated portion of the ~~DoDIN~~*DODIN* in accordance with Reference (~~by~~*bx*), Committee on National Security Systems Instruction (CNSSI) No. 1010 (Reference (~~bz~~*by*)), and as described in NIST SP 800-61 (Reference (~~ea~~*bz*).

b. Ensures the acquisition and preservation of copies of digital media, logs, and investigative and technical data associated with cyber intrusion incidents, investigations, and operations required for tactical analysis, strategic analysis, or law enforcement investigations in accordance with Reference (~~ea~~*bz*).

c. Requires DoD Components to report all incidents that appear to be violations of federal law to DoD Component defense criminal investigative organizations; law enforcement organizations; and the IG DoD. Incidents involving cleared defense contractors will be reported to DSS as described in Reference (k) and DoDD 5240.06 (Reference (~~cb~~*ca*)).

d. Requires DoD Components to develop, implement, and enforce procedures to prevent, handle, isolate, contain and mitigate incidents involving the unauthorized disclosure of classified and CUI in accordance with References (~~be~~*bd*), (~~bf~~*be*), (~~bg~~*bf*), and (~~by~~*bx*); CNSSP No. 18 (Reference (~~ee~~*cb*)); and CNSSI No. 1001 (Reference (~~ed~~*cc*)).

7. ~~DoDIN~~*DODIN* UAM FOR DoD INSIDER THREAT PROGRAM. ~~DoDIN~~*DODIN* user monitoring capability and system auditing capability will support UAM to detect, deter, and mitigate insider threats. The UAM information compiled from these sources, integrated with information from various other sources (e.g., human resources, law enforcement, and counterintelligence) supports analysis and response to counter insider threats on the ~~DoDIN~~*DODIN*. The DoD Insider Threat Program's UAM:

a. Requires a user monitoring capability and auditing capability to identify and evaluate anomalous activity by ~~DoDIN~~*DODIN* users for the DoD Insider Threat Program in accordance with Reference (~~y~~*x*). The development and implementation of these capabilities supports UAM and requires coordination between the USD(I), USD(P), USD(P&R), USD(AT&L), and DoD CIO.

b. Implements minimum standards for UAM in accordance with References (~~y~~*x*) and (~~z~~*y*). This includes procedures to maintain audit data and preserve audit data chain of custody.

c. Establishes procedures for responding to anomalous user activity on the ~~DoDIN~~*DODIN*, including procedures to mitigate potential damage to data on the ~~DoDIN~~*DODIN* and to contact applicable DoD Component investigative authority when necessary in accordance with References (~~y~~*x*) and (~~by~~*bx*) and DoDD 5240.26 (Reference (~~ee~~*cd*)).

8. WARNING INTELLIGENCE AND AS&W. Warning intelligence activities are intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intentions against U.S. partners or interests as described in JP 2-0 (Reference (~~ef~~*ce*)). AS&W can provide detection and reporting of time-sensitive information on developments that could involve a threat to the enterprise system or provide the enterprise a warning that an attack is happening. This would include the detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed. Warning intelligence and AS&W information:

a. Provides the capability to receive notice of AS&W and warning intelligence information provided by intelligence organizations such as DIA and the National Security Agency.

b. Supports analysis of threats, suspicious or malicious network traffic, and attacks.

c. Enables the DoD Components to prevent or mitigate impact to the DoD Component-owned or -operated portion of the ~~DoDIN~~*DODIN*.

9. <u>ACCOUNTABILITY</u>

a. Individuals and organizations will be held accountable for implementing DoD Component activities outlined in this enclosure, including actions directed by DoD Component heads to protect the ~~DoDIN~~*DODIN*. This includes:

(1) Commanders, authorizing officials, information system security managers, information system security officers, program managers, project and application leads, supervisors, network administrators, systems administrators, and users responsible for implementing directed actions.

(2) DoD Component internal or external cybersecurity service providers who are responsible for implementing cybersecurity services in accordance with DoD Component policy, MOAs, contracts, or support agreements such as a DD Form 1144, "Support Agreement" in accordance with Reference (m).

b. Actions may be taken against military and civilian personnel who knowingly, willfully, or negligently compromised, damaged, or placed at risk systems by not ensuring implementation of DoD system security requirements in accordance with this instruction; References (h) and (~~be~~*bd*); and supplemental DoD Component policies and procedures.

c. Defense contractors are responsible for ensuring their employees perform under the terms of the contract and applicable directives, laws, and regulations, and must maintain employee discipline. The contracting officer, or designee, is the liaison with the defense contractor for directing or controlling contractor performance in accordance with the contract. Outside of the assertion of criminal jurisdiction for misconduct, the contractor is responsible for disciplining contractor personnel. Criminal jurisdiction within the United States could be asserted by Federal, State, or local authorities. For defense contract personnel integrated into contingency operations outside the United States, see Reference (~~bl~~*bk*).

d. In order to hold individuals accountable, DoD Components must ensure that they receive required training and certifications for their positions and understand their responsibilities in accordance with References (h) and (~~be~~*bd*); DoDD 8140.01 (Reference (~~eg~~*cf*)); and additional DoD Component training or certification requirements.

ENCLOSURE 4

CYBERSECURITY INTEGRATION INTO ~~DoDIN~~*DODIN* OPERATIONS

1. CYBERSECURITY ACTIVITIES INTEGRATION

   a. DoD Components will organize and integrate cybersecurity activities to support ~~DoDIN~~*DODIN* operations and DCO internal defensive measures consistent with published orders and directives.

   b. DoD Component subordinate organizations and authorizing officials responsible for systems will comply with orders or directives from CDRUSSTRATCOM and their DoD Component authority designated to direct the security, operations, and defense of the DoD Component's portion of the ~~DoDIN~~*DODIN*.

   c. Figure 1 represents the flow of information between organizations to implement directed ~~DoDIN~~*DODIN* operations and DCO internal defensive measures. DoD requires horizontal and vertical ~~DoDIN~~*DODIN* situational awareness across DoD organizations. The figure shows the transition to JIE with the placement of enterprise operations centers (EOCs), core data centers, installation processing nodes, installation services nodes, and special purpose processing nodes described in Reference (d).

Figure 1. ~~DoDIN~~*DODIN* Operations, DCO Internal Defensive Measures, and Situational Awareness
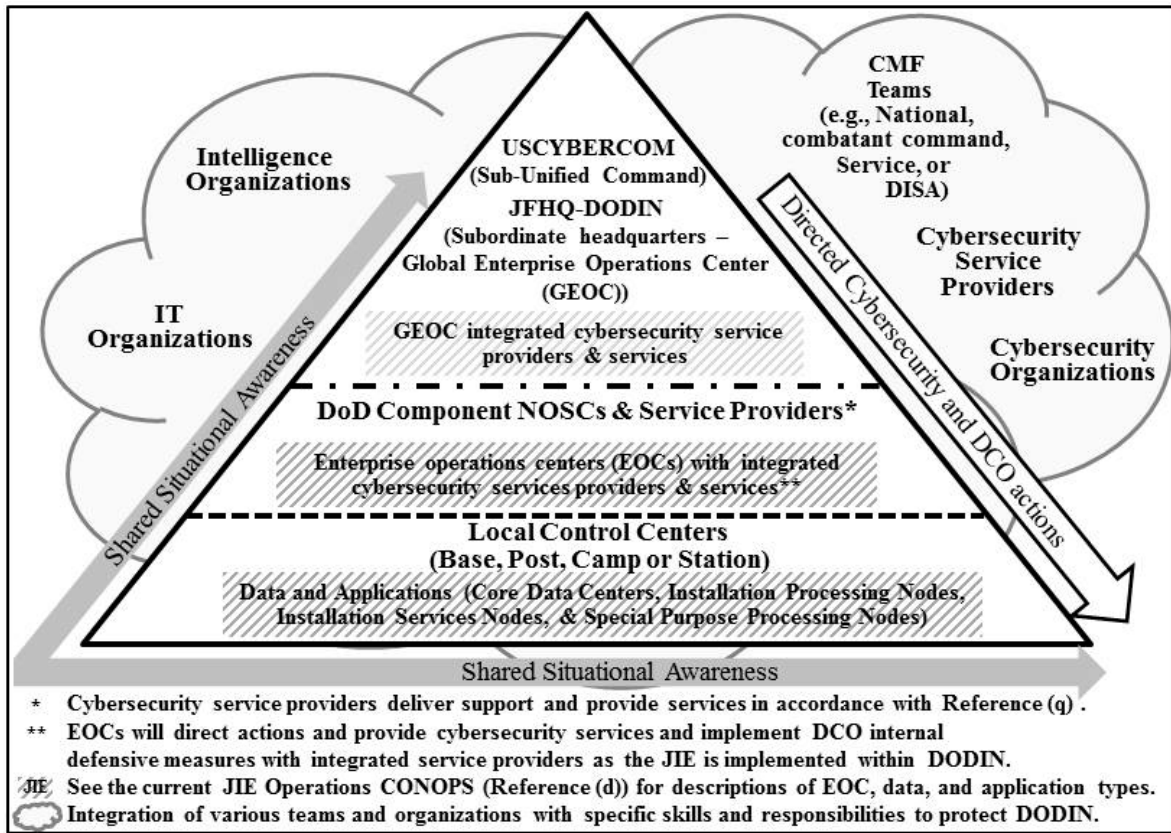
2. CYBERSECURITY ACTIVITIES TO PROTECT THE ~~DoDIN~~*DODIN*. The DoD Component-owned or -operated portion of the ~~DoDIN~~*DODIN* will be aligned with a NOSC and an integrated capability to conduct cybersecurity activities. This cybersecurity capability may be obtained from within a DoD Component or from an authorized external DoD Component service provider. All service providers must be authorized in accordance with Reference (~~q~~*p*).

    a. The system owners and authorizing officials will comply with actions directed from their aligned NOSC using internal cybersecurity organizations and supporting cybersecurity service providers. Figure 2 provides a view of the alignment of systems and relationships between current DoD Component NOSC, USSTRATCOM, and the transition to the JIE as described in in Reference (d).

Figure 2. Notional View of Current and Future Integration of Cybersecurity Activities
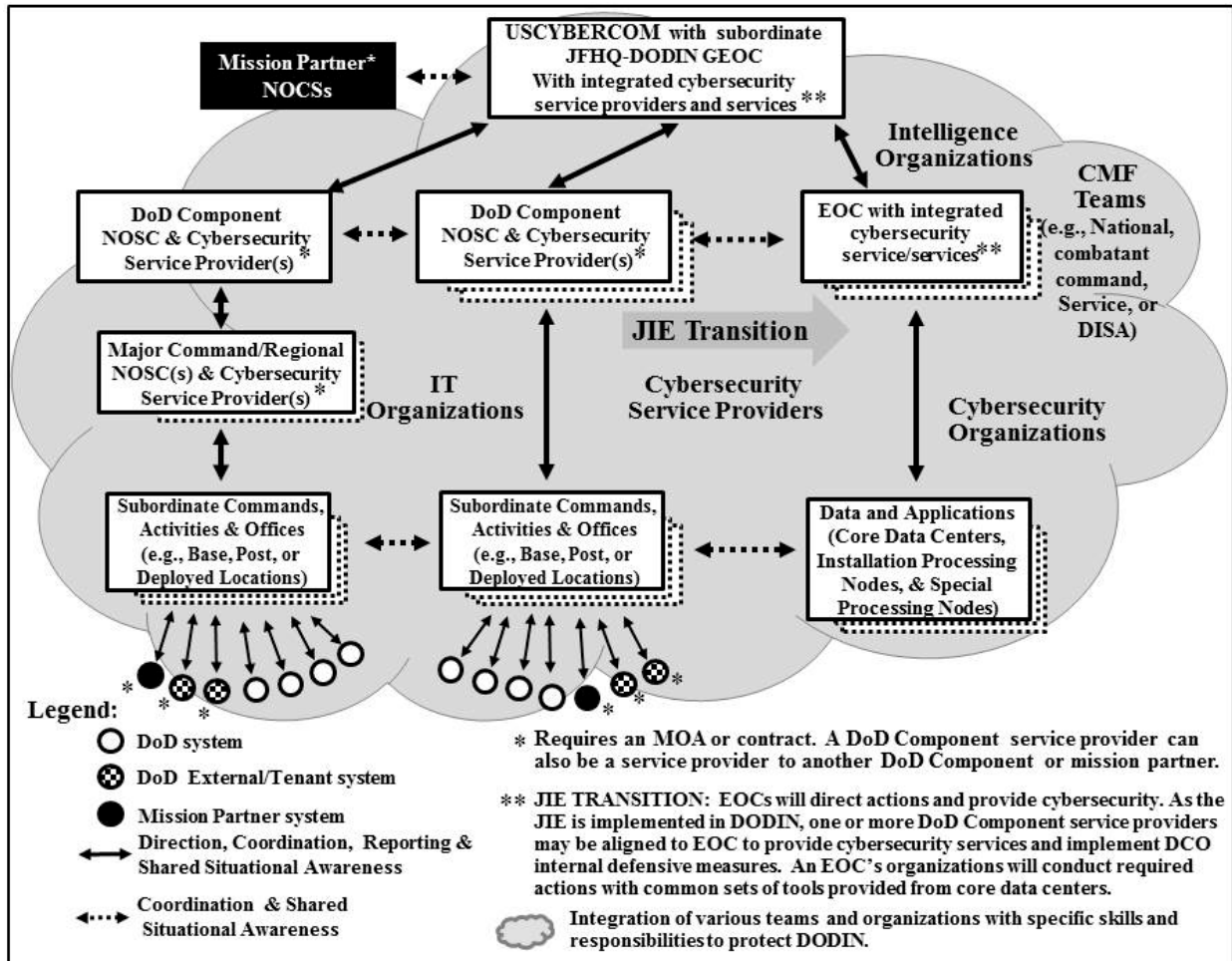
(1) Actions will be implemented as directed by the joint or DoD Component NOSC in accordance with CDRUSSTRATCOM and DoD Component orders and directives.

(2) Cybersecurity services may be provided to an individual system by one or more cybersecurity service providers through a NOSC.

(3) The owner or operator of a system that does not have connectivity to the ~~DoDIN~~*DODIN* must have processes to receive orders and directives, report compliance with directed actions, and provide the capability to exchange information and reporting on the security status of the system through the appropriate DoD Component headquarters.

   b. The cybersecurity service provider responsibilities and the subscriber responsibilities for each cybersecurity service provided will be specifically assigned and documented.

(1) These cybersecurity service provider and subscriber responsibilities will be documented in a support agreement, MOA, contract, or in accordance with applicable DoD Component issuance (e.g., CONOPs).

(2) Cybersecurity services provided will be aligned with applicable security controls. The implemented security controls will be documented in the support agreement, MOA, or contract.

(3) The cybersecurity service subscriber will ensure the use of appropriate controls and oversight measures with respect to agreements.

c. DoD Component organizations that own or operate or have operated on their behalf systems have ultimate responsibility for the security of their systems and will be held accountable for leveraging findings from readiness inspections. Although the cybersecurity service provider is responsible for a specific set of cybersecurity services, in certain areas the primary responsibility for cybersecurity activities may still remain with the DoD system owner to implement actions in accordance with the documented support agreement. DoD Component organizations that own or operate systems:

(1) Will validate that support agreements are comprehensive and define organizational roles and responsibilities and the scope and applicability of the cybersecurity service(s) to be provided by the DoD cybersecurity service providers, including those provided to tenant organizations.

(2) Will establish and maintain records identifying cybersecurity service provider(s) and cybersecurity services provided to their organization, including the DoD Component portions of the ~~DoDIN~~*DODIN* or specified system serviced; GENSER or SE designations; authorizing official; mission criticality; internet protocol address ranges; and the corresponding physical location for each owned or operated system including those operated on behalf of the DoD Component organization by a mission partner.

(3) Must register these systems in accordance with their DoD Component guidance and will be held accountable if found not aligned with a DoD Component or external NOSCs and supporting cybersecurity service provider(s).

(4) Will monitor the effectiveness of cybersecurity services provided by either a DoD Component or an external cybersecurity service provider. Issues that cannot be resolved concerning support agreement responsibilities will be reported to their DoD Component CIO.

(5) Will verify POA&Ms to correct deficiencies or weaknesses identified during evaluations or inspections by the DoD Component or by external organizations such as CDRUSSTRATCOM; Director, DISA; DIRNSA/CHCSS; or Director, DIA, are maintained by the DoD Component. POA&Ms and subsequent updates will be provided to CDRUSSTRATCOM and Director, DISA, for GENSER systems, and Director, DIA, for SE systems as required.

(6) Will report cybersecurity service provider changes through their DoD Component head to CDRUSSTRATCOM and Director, DISA, for GENSER systems or to Director, DIA, for SE systems.

(7) Will forward issues between DoD Components that cannot be resolved on the implementation of cybersecurity services or alignment of cybersecurity service providers through the DoD Component CIO to the DoD CIO or to the CJCS, as appropriate.

(8) Will submit the evaluation request package for cybersecurity services through the DoD Component headquarters in accordance with Reference (~~q~~*p*).

(9) May, if currently authorized to provide GENSER or SE cybersecurity services, submit a reciprocity request for evaluation to provide GENSER and SE cybersecurity services in accordance with Reference (~~q~~*p*).

(a) Evaluation of requests to provide reciprocal cybersecurity services will encompass a review of current evaluation documentation and an evaluation of areas not covered in current documentation as the basis to recommend authorization to provide additional GENSER or SE cybersecurity services.

(b) Authorization to provide GENSER and SE cybersecurity services will be coordinated between the CDRUSSTRATCOM, the Director, DISA, and the Director, DIA.

d. DoD Component organizations will establish a contract, MOA, support agreement, or international agreement with a mission partner that identify specific interconnection ~~DoDIN~~*DODIN* operations responsibilities between the DoD Component and mission partner; the cybersecurity requirements for mission partner systems; and protection requirements for DoD data resident on mission partner systems.

(1) Capabilities and requirements for activities outlined in Enclosure 3 must be incorporated into formal agreements based on:

(a) A DoD Component risk assessment.

(b) DoD risk tolerance guidance provided by the DoD risk executive in accordance with Reference (f).

(c) Applicable Federal, DoD, and DoD Component policy and regulations on DoD CIO authorized interconnection of mission partner systems to the ~~DoDIN~~*DODIN*, including the DISA Connection Process Guide (Reference (~~ch~~*cg*)) and CDRUSSTRATCOM orders or other directives issued through CDRUSCYBERCOM.

(2) Classified information processed and stored on contractor systems will be in accordance with:

(a) References (h) and (k).

(b) The required contract cybersecurity requirements clause in accordance with DoD 5220.22-R (Reference (ci)).

(c) Subpart 4.4 of the Federal Acquisition Regulation (Reference (cj)) for contractors operating under the NISP.

(3) Unclassified DoD information in the possession or control of non-DoD entities on non-DoD systems will have adequate cybersecurity requirements provided through all contracts, grants, or other legal agreements in accordance with DoDI 8582.01 (Reference (ck)). DoD unclassified controlled technical information resident on or transiting through DoD contractor project, enterprise, or company-wide unclassified information technology system(s), of non-DoD entities on non-DoD systems will have adequate cybersecurity requirements in accordance with Defense Federal Acquisition Regulation Supplement Clause 252.204-7012 (Reference (cl)).

(4) Mission partners will be required by contract, MOA, support agreement, or international agreement to meet cybersecurity requirements or obtain cybersecurity services in order to connect to the ~~DoDIN~~*DODIN*.

(a) DoD Component contracts will require Defense contractors to meet cybersecurity requirements or obtain cybersecurity services in order to connect to the ~~DoDIN~~*DODIN* in accordance with Reference (ch).

(b) Support agreements such as an MOA established in collaboration with the DoD CIO will require federal mission partners directly connected to the ~~DoDIN~~*DODIN* to subscribe to a DoD cybersecurity service provider, or establish their own equivalent cybersecurity service capability assessed by the DoD CIO and Director, DISA, as compliant with or equivalent to Reference (~~q~~*p*) requirements, applicable Committee on National Security Systems (CNSS) requirements, and NIST guidelines.

(c) Federal mission partners connecting to the ~~DoDIN~~*DODIN* via a DoD CIO approved DMZ will be responsible for protecting their information networks in accordance with CNSS requirements. The DoD CIO approved DMZs provide cybersecurity services to protect, monitor, detect, and respond to potential attacks on the ~~DoDIN~~*DODIN* via the DMZs. Federal mission partners may request that DISA provide cybersecurity services for their interconnection to a DoD CIO approved DMZ on a subscription basis.

(d) Negotiation and conclusion of international agreements for interconnection with mission partners that are allies, coalition members, host nations and other nations, and multinational organizations will be subject to and consistent with Reference (n).

(5) Mission partner DMZ or point-to-point interconnections to the ~~DoDIN~~*DODIN* will be in accordance with Reference (ch).

(6) Mission partner interconnections with the ~~DoDIN~~*DODIN* must have validated requirements approved by a sponsoring DoD Component and the DoD CIO.

(a) Sponsors will ensure all connection request fulfillment actions are completed.

(b) Sponsors will complete or assist the non-DoD mission partner with providing appropriate authorization package in accordance with References (f), (h), and (ci); as described in Reference (~~bw~~*bv*); or other applicable guidance for a specific mission partner interconnection.

3. <u>CYBERSECURITY SERVICE PROVIDERS</u>

a. The DoD Components will:

(1) Support evaluation of DoD Component cybersecurity service providers' services in accordance with Reference (~~q~~*p*). For an organization not evaluated and authorized to provide cybersecurity services, forward a request for evaluation to DISA or DIA in accordance with Reference (~~q~~*p*).

(2) Oversee DoD Component cybersecurity service provider(s) development and publication of cost models, as required, for providing cybersecurity services to protect DoD Component or externally owned or operated systems connected to the ~~DoDIN~~*DODIN* through a support agreement, MOA, or contract.

(3) Measure the effectiveness of cybersecurity service provider services provided in accordance with support agreements, MOAs, or contracts. Resolve issues that cannot be resolved between a DoD Component cybersecurity service provider and the external subscribers, as required.

b. The DoD CIO Cybersecurity Service Provider Process Manager will:

(1) Maintain guidance to evaluate the maturity level of DoD cybersecurity service providers to provide services in accordance with Reference (~~q~~*p*).

(2) Develop, implement, and maintain a process to validate Federal mission partner capability to provide equivalent cybersecurity services and evaluate the risk to the ~~DoDIN~~*DODIN*.

(3) Validate the designation of the systems either as SE or GENSER, as defined in the Glossary.

(4) Maintain a list of DoD GENSER and SE cybersecurity service providers authorized to provide cybersecurity services, in coordination with the CDRUSSTRATCOM; the Director, DIA; and the Director, DISA.

c. Cybersecurity service providers will:

(1) Offer and provide cybersecurity services in accordance with Reference (~~q~~*p*).

(2) Execute cybersecurity responsibilities and authorities in accordance with DoD Component policy, MOAs, contracts, or support agreements.

(3) Comply with directives and orders of USSTRATCOM and supported DoD Component NOSC and organizations.

(4) Document all supported entities and associated systems in accordance with DoD Component policy, MOAs, contracts, or support agreements.

4. DoD CIO CYBERSECURITY ARCHITECT. The DoD CIO Cybersecurity Architect:

a. Oversees development DoD cybersecurity architectures to support protection of the DoDIN*DODIN* in coordination with DoD Components.

b. Advises DoD Components' cybersecurity architects and capabilities boards, panels, and working groups on:

(1) Architecture priorities as related to the DoD cybersecurity reference architecture.

(2) Enterprise capability gaps that require operational and technical requirements and solutions development.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AS&W	attack sensing and warning
ASD(R&E)	Assistant Secretary of Defense for Research and Engineering
CDRUSCYBERCOM	Commander, United States Cyber Command
CDRUSSTRATCOM	Commander, United States Strategic Command
CIO	Chief Information Officer
CIMB	Cyber Investment Management Board
CJCS	Chairman of the Joint Chiefs of Staff
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CMF	Cyber Mission Forces
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CONOPS	concept of operations
CUI	controlled unclassified information
DACO	directive authority for cyberspace operations
DCO	defensive cyberspace operations
DIA	Defense Intelligence Agency
DIRNSA/CHCSS	Director National Security Agency/Chief Central Security Service
DISA	Defense Information Systems Agency
DMZ	demilitarized zone
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
~~DoDIN~~*DODIN*	DoD information network
~~DoDIN~~*DODIN* operations	DoD information network operations
DoDM	DoD Manual
DOT&E	Director, Operational Test and Evaluation
DSS	Defense Security Service

EOC	enterprise operations center
EXORD	execute order
FED	federal
FISMA	Federal Information Security Modernization Act
GC, DoD	General Counsel of the Department of Defense
GENSER	general service
IC	intelligence community
ICS	industrial control system
IG DoD	Inspector General of the Department of Defense
IR	intelligence requirement
ISCM	Information Security Continuous Monitoring
ISCMWG	Information Security Continuous Monitoring Working Group
JCIDS	Joint Capabilities Integration and Development System
JFHQ- ~~DoDIN~~*DODIN*	Joint Force Headquarters- ~~DoDIN~~*DODIN*
JIE	Joint Information Environment
JP	Joint Publication
JWICS	Joint Worldwide Intelligence Communications System
MOA	memorandum of agreement
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NOSC	network operations and security center
NSS	national security system
OPFOR	opposing force
OPORD	operation order
PCA	Principal Cyber Advisor
PIT	platform information technology
POA&M	plan of action and milestones

REL	releasable
RMF	Risk Management Framework
SAP	special access program
SCI	sensitive compartmented information
SE	special enclave
SP	Special Publication
TASKORD	tasking order
UAM	user activity monitoring
USCG	*United States Coast Guard*
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
USD(P&R)	Under Secretary of Defense for Personnel and Policy
USSTRATCOM	United States Strategic Command

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this instruction.

AS&W. Defined in CNSSI No. 4009 (Reference (~~em~~*cl*)).

continuous monitoring. Defined in Reference (~~em~~*cl*).

control system. Defined in Reference (i)

cybersecurity. Defined in Reference (h).

cybersecurity service. A service provided or subscribed to in order to protect the ~~DoDIN~~*DODIN*. Cybersecurity services include capabilities to implement DoD Component activities addressing vulnerability assessment and analysis; vulnerability management; malware protection; continuous monitoring; incident handling; insider threat process to identify and evaluate anomalous user activity; and warning intelligence and AS&W to protect the ~~DoDIN~~*DODIN*.

cybersecurity service provider. An organization that provides one or more cybersecurity services to implement and protect the ~~DoDIN~~*DODIN*.

cyberspace. Defined in ~~JP 1-02~~ *the DoD Dictionary of Military and Associated Terms* (Reference (~~en~~*cm*)).

cyberspace operations. Defined in Reference (~~en~~*cm*).

defensive cyberspace operations. Defined in Reference (~~en~~*cm*).

DACO. Directive authority for the purpose of issuing orders to DoD Components in order to assure the effective functioning and defense of the entire DoDIN.

~~DoDIN~~*DODIN*. Defined in Reference (~~en~~*cm*).

~~DoDIN~~*DODIN* operations. Defined in Reference (~~en~~*cm*).

~~DoDIN~~*DODIN* situational awareness. An environment where ~~DoDIN~~*DODIN* operations, internal defensive measures, vulnerability, and adversary threat information can be shared in real time to provide actionable information between enterprise operations centers, network operations and security centers, cybersecurity service providers, and mission partners. ~~DoDIN~~*DODIN* operations activities and situational awareness of these activities are the foundation of cyberspace situational awareness. ~~DoDIN~~*DODIN* operations are fundamental to the commander's situational awareness of the operational environment as described in Reference (e).

GENSER. Unclassified or classified systems that are not subject to the enhanced security protections (e.g., safeguarding, access requirements) required for SCI or special access program (SAP) information.

ICS. Defined in Reference (i).

ISCM. Defined in Reference (~~em~~*cl*).

incident handling. Defined in Reference (~~em~~*cl*).

information system. Defined in Reference (~~em~~*cl*).

insider threat. Defined in Reference (~~em~~*cl*).

internal defensive measures. Actions to dynamically reestablish, re-secure, reroute, reconstitute, or isolate degraded or compromised ~~DoDIN~~*DODIN* in response to unauthorized activity or alert and threat information.

malicious applets. Small application programs automatically downloaded and executed that perform an unauthorized function on an information system.

malicious code. Defined in Reference (~~em~~*cl*).

malicious logic. Defined in Reference (~~em~~*cl*).

malware. Defined in Reference (~~em~~*cl*).

mission partners. Defined in Reference (~~t~~*s*).

NOSC. The term NOSC will be used generically in this instruction for the various types and names used for network operations and security centers organized by joint or DoD Components to direct and manage operations and cybersecurity activities to protect the ~~DoDIN~~*DODIN*, including JIE enterprise operations centers (EOCs).

NSS. Defined in Reference (~~em~~*cl*).

penetration testing. Defined in Reference (~~em~~*cl*).

PIT system. Defined in Reference (h).

RMF. Defined in Reference (~~em~~*cl*).

red team. Defined in Reference (~~em~~*cl*).

risk tolerance. Defined in Reference (~~em~~*cl*).

SE. Systems with special security requirements, such as a SAP, special access requirements, or SCI.

situational awareness. Cyberspace situational awareness is the requisite current and predictive knowledge of cyberspace and the operational environment upon which cyberspace operations depend including factors affecting friendly and adversary cyberspace forces. Also see ~~DoDIN~~*DODIN* situational awareness.

spillage. Defined in Reference (~~em~~*cl*).

unauthorized disclosure. Defined in Reference (~~em~~*cl*).

vulnerability. Defined in Reference (~~em~~*cl*).

vulnerability assessment. Defined in Reference (~~em~~*cl*).

warning intelligence. Defined in Reference (~~en~~*cm*).