



DEPUTY SECRETARY OF DEFENSE  
1010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1010

June 21, 2017  
Incorporating Change 3, May 29, 2020

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Directive-Type Memorandum (DTM) 17-007 – “Interim Policy and Guidance for Defense Support to Cyber Incident Response”

References: See Attachment 1.

Purpose. This DTM:

- Provides supplementary policy guidance, assigns responsibilities, and details procedures for providing Defense Support to Cyber Incident Response (DSCIR).
- Is effective June 21, 2017. This DTM will expire June 21, 2021 and will be converted to a new issuance in accordance with DoD Instruction (DoDI) 5025.01.

Applicability. This DTM:

- Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within DoD (referred to collectively in this DTM as the “DoD Components”).
- Applies to the Army National Guard and the Air National Guard (referred to collectively in this DTM as the “National Guard”) personnel when under federal command and control. Also applies to National Guard personnel when:
  - The Secretary of Defense determines that it is appropriate to employ National Guard personnel in Title 32, United States Code (U.S.C.), status to fulfill a request for defense support of civil authorities.
  - The Secretary of Defense requests the concurrence of the governors of the affected States.
  - Those governors concur in the employment of National Guard personnel in such a status.
- In addition to the “does **not** apply” provisions in Section 2.d. of DoD Directive (DoDD) 3025.18, this DTM does not apply to:

- Assistance incidental to military training (see Section 2012 of Title 10, U.S.C.)
- Activities conducted in accordance with the May 24, 2016, Deputy Secretary of Defense Policy Memorandum 16-002.
- Offensive cyberspace operations.
- Defensive cyberspace operations-response actions.
- The exchange of information among mission partners conducted in accordance with DoDI 8110.01.
- DoD Cyber Crime Center activities in accordance with DoDD 5505.13E.
- DoD cybersecurity partnership activities with the Defense Industrial Base in accordance with DoDI 5205.13.
- Computer incident notifications to the Department of Homeland Security U.S. Computer Emergency Readiness Team (USCERT) consistent with the USCERT Federal Incident Notification Guidelines.
- Policies and procedures referenced in National Security Directive 42.
- National Guard activities conducted in State active duty status, including State immediate response activities using National Guard personnel (as described in Section 4.2(h) of DoDD 3025.18), activities that are determined to be the responsibilities of the individual States, or activities conducted through the execution of mutual aid and assistance agreements between the States or local civil authorities.

Definitions. See Glossary.

Policy. It is DoD policy that:

- This DTM will be implemented consistent with national security objectives and military readiness. DoD will, at all times, remain postured to perform priority military missions in cyberspace at the direction of the President or the Secretary of Defense.
- DSCIR is provided within the framework of Defense Support of Civil Authorities, as defined in DoDD 3025.18.
- DSCIR is planned, provided, and executed:
  - In accordance with the policies, procedures, and responsibilities in this DTM and DoDD 3025.18.
  - In accordance with Presidential Policy Directive (PPD)-41 and other appropriate laws and policies, DoD supports the lead federal departments and agencies for asset and threat response to cyber incidents outside the DoD Information Network (DoDIN).

- In accordance with Section 1835 of Title 18, U.S.C. (also known as “the Posse Comitatus Act”) and Section 275 of Title 10, U.S.C.
- In accordance with Section 552a of Title 5, U.S.C. (also known and referred to in this DTM as “the Privacy Act of 1974, as amended”).
- Requests for DSCIR will be evaluated consistent with the criteria established in DoDD 3025.18, with emphasized consideration given, but not limited to, the impact on DoD networks, systems, and capabilities if the support were to be provided.
- DSCIR may include direct on-location support, remote support, or a combination of both as appropriate.
- Requests for assistance for DSCIR will be considered only if they include:
  - Written acknowledgment that the entity receiving federal support understands that the federal support may include DoD support, which would be provided through the lead federal agency.
  - Written permission for DoD to access appropriate information and information systems (e.g., applicable hardware, software, networks, servers, IP addresses, and databases).
- When a request for DSCIR is received and approved, it is done so as prescribed in the June 28, 2016, Deputy Secretary of Defense memorandum, DoDD 3025.18, and DoDI 3025.21.
- DSCIR to save lives, prevent human suffering, or mitigate great property damage may be provided under immediate response authority in accordance with DoDD 3025.18, but only in response to a request for assistance from a lead federal department or agency for asset response or threat response outside the DoDIN (as described in PPD-41).
  - Aforementioned acknowledgments and permissions may be oral when immediate response is requested and sufficient time is not available for written documentation before providing DSCIR.
  - However, oral acknowledgments and permissions must be documented by the authorizing DoD official and must be followed by written acknowledgments and permissions from the requestors at the earliest available opportunity.
- DSCIR may be provided using DoD military personnel, DoD civilian personnel, and DoD contractor personnel. The use of National Guard personnel for DSCIR in a duty status pursuant to Section 502(f) of Title 32, U.S.C., will be considered consistent with DoDD 3025.18, DoDI 3025.22, and this DTM.
- As appropriate, and based on the nature of the support, any liability waivers, memorandums of understanding, memorandums of agreement, non-disclosure

agreements, or other appropriate legal documents requested by DoD must be signed before providing DSCIR.

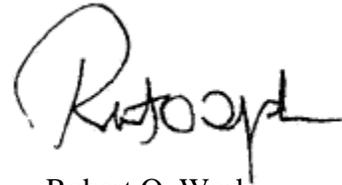
Responsibilities. Attachment 2 provides responsibilities for implementing this DTM.

Procedures. Attachment 3 provides mandatory procedures for complying with this DTM.

Information Collections. The situational and after-action reports, referred to in Paragraph 12.g. of Attachment 2 of this DTM, do not require licensing with a report control symbol in accordance with Paragraph 1.b(5) of Enclosure 3 of Volume 1 of DoD Manual 8910.01.

Releasability. **Cleared for public release.** This DTM is available on the Directives Division Website at <http://www.esd.whs.mil/DD/>.

Summary of Change 3. The expiration date of this DTM was extended.



Robert O. Work

Deputy Secretary of Defense

Attachments:  
As stated

**DISTRIBUTION:**

Secretaries of the Military Departments  
Chairman of the Joint Chiefs of Staff  
Under Secretaries of Defense  
Deputy Chief Management Officer  
Chief of the National Guard Bureau  
General Counsel of the Department of Defense  
Director, Cost Assessment and Program Evaluation  
Inspector General of the Department of Defense  
Director, Operational Test and Evaluation  
Chief Information Officer of the Department of Defense  
Assistant Secretary of Defense for Legislative Affairs  
Assistant to the Secretary of Defense for Public Affairs  
Director, Strategic Capabilities Office  
Director, Net Assessment  
Directors of the Defense Agencies  
Directors of the DoD Field Activities

ATTACHMENT 1

REFERENCES

Deputy Secretary of Defense Memorandum, "Delegation of Approval Authority," June 28, 2016  
Deputy Secretary of Defense Policy Memorandum 16-002, "Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities," May 24, 2016  
Deputy Secretary of Defense Memorandum, "Principal Cyber Advisor Roles and Responsibilities," December 19, 2016  
DoD 5400.7-R, "DoD Freedom of Information Act (FOIA) Program," January 25, 2017  
DoD 7000.14-R, "Department of Defense Financial Management Regulation," date varies by volume  
DoD Directive 1322.18, "Military Training," January 13, 2009  
DoD Directive 3025.18, "Defense Support of Civil Authorities (DSCA)," December 29, 2010, as amended  
DoD Directive 5105.77, "National Guard Bureau (NGB)," October 30, 2015  
DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)), " October 24, 2014, as amended  
DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992  
DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014  
DoD Directive 5505.13E, "DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)," March 1, 2010  
DoD Directive S-5210.36, "Provision of DoD Sensitive Support to DoD Components and Other Departments and Agencies of the U.S. Government (U)," November 6, 2008, as amended<sup>1</sup>  
DoD Instruction 1215.06, "Uniform Reserve, Training and Retirement Categories for the Reserve Components" March 11, 2014, as amended  
DoD Instruction 3025.21, "Defense Support of Civilian Law Enforcement Agencies," February 27, 2013  
DoD Instruction 3025.22, "The Use of the National Guard for Defense Support of Civil Authorities," July 26, 2013  
DoD Instruction 5025.01, "DoD Issuances Program," August 1, 2016  
DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016  
DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cybersecurity/Information Assurance (CS/IA) Activities," January 29, 2010  
DoD Instruction 8110.01, "Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD," November 25, 2014  
DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

---

<sup>1</sup> This document is classified and not releasable to the public. Individuals may request access to this document from the Office of the Under Secretary of Defense for Intelligence, through the Heads of their OSD Components

DoD Manual 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information,” February 24, 2012

DoD Manual 8910.01, Volume 1, “DoD Information Collections: Procedures for DoD Internal Information Collections,” June 30, 2014, as amended

Executive Order 12333, “United States Intelligence Activities,” December 4, 1981, as amended

Executive Order 13526, “Classified National Security Information,” December 29, 2009, as amended

Joint Publication 3-28, “Defense Support of Civil Authorities,” July 31, 2013

National Security Directive-42, “National Policy for the Security of National Security Telecommunications and Information Systems,” July 5, 1990

National Institute of Standards and Technology Interagency 7298 Revision 2, “Glossary of Key Information Security Terms,” 31 May 2013

National Disclosure Policy No. 1, “National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations,” October 1, 1988.

Office of the Chairman of the Joint Chiefs of Staff, “DoD Dictionary of Military and Associated Terms,” current edition

Secretary of Defense Memorandum, “Global Force Management Implementation Guidance,” current edition.<sup>2</sup>

Unified Command Plan, current edition.

United States Code, Title 5, Section 552a (also known as “the Privacy Act of 1974, as amended”)

United States Code, Title 10

United States Code, Title 18, Section 1835 (also known as “the Posse Comitatus Act”)

United States Code, Title 31, Section 1535 (also known as “the Economy Act”)

---

<sup>2</sup> This document is classified and not releasable to the public. Individuals may request access to this document from the Office of the Under Secretary of Defense for Policy, through the Heads of their OSD Components.

ATTACHMENT 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P):

- a. Coordinates DSCIR policy with the DoD Components, and consults with other federal departments and agencies and State governments as appropriate.
- b. Establishes DoD policy governing DSCIR.

2. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY (ASD(HD&GS)). Under the authority, direction, and control of the USD(P) and as the principal advisor to the USD(P) and the Secretary of Defense on cyberspace policy matters and defense support of civil authorities, the ASD(HD&GS):

- a. Serves as the principal civilian advisor for DSCIR.
  - b. Approves requests for DSCIR in accordance with the June 28, 2016, Deputy Secretary of Defense memorandum, DoDD 3025.18, DoDI 3025.21, and this DTM. When carrying out this authority, the ASD(HD&GS) will:
    - (1) Coordinate with the Chairman of the Joint Chiefs of Staff (CJCS), the Combatant Commanders, the General Counsel of the Department of Defense, the DoD Chief Information Officer (CIO), the USD(I), and other DoD officials as appropriate.
    - (2) Immediately notify the Secretary of Defense of the use of this authority.
    - (3) Notify the Secretary of Defense before approving DSCIR requests that would benefit private sector entities or non-governmental organizations.
  - c. Develops, coordinates, and oversees the implementation of DoD policy for DSCIR plans and activities consistent with the policies in PPD-41, including the coordination or consultation, as appropriate, with the Department of Homeland Security, the Department of Justice, and other appropriate federal departments and agencies on the development and validation of DSCIR requirements.
  - d. Ensures that DSCIR plans and activities are consistent with Section 1535 of Title 31, U.S.C. (also known as “the Economy Act”) and other appropriate laws and policies.
  - e. Before a cyber incident, to the extent practicable and in coordination with the General Counsel of the Department of Defense, the DoD CIO, the CJCS, and other DoD officials as appropriate:

(1) Develops approval agreements with other federal departments and agencies to expedite DSCIR in response to a time-sensitive cyber incident or other threat that requires DoD support.

(2) Submits agreements to the Secretary of Defense for approval.

f. As the Defense Domestic Crisis Manager, serves as the principal representative to the Cyber Response Group. Through the Cyber Response Group, identifies the representatives to the Unified Coordination Group in accordance with PPD-41.

3. DOD PRINCIPAL CYBER ADVISOR. The DoD Principal Cyber Advisor serves as the primary official under the Secretary and Deputy Secretary of Defense to synchronize and coordinate issues related to DoD forces and activities as outlined in the December 19, 2016, Deputy Secretary of Defense memorandum.

4. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE. The Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense establishes policies and procedures to ensure timely reimbursement to DoD for reimbursable DSCIR activities.

5. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R) identifies, monitors, and oversees the development of integrated DSCIR cyber capabilities and training capabilities and the integration of these training capabilities into exercises and training to build, sustain, and assess DSCIR readiness in accordance with DoDD 1322.18.

6. ASSISTANT SECRETARY OF DEFENSE FOR MANPOWER AND RESERVE AFFAIRS. Under the authority, direction, and control of the USD(P&R), the Assistant Secretary of Defense for Manpower and Reserve Affairs provides to the ASD(HD&GS) recommendations, guidance, and support on the use of the Reserve Components to perform DSCIR missions.

7. DoD CIO. The DoD CIO:

a. Notifies the USD(P), when requested by mission partners, to provide cyber incident response support.

b. Coordinates with the USD(P) on the planning and provision of cyber incident response support to mission partners.

8. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), in accordance with DoDD 5143.01 and DoDD S-5210.36:

a. Notifies the ASD(HD&GS) of all requests for technical assistance received by NSA from a non-DoD entity in response to a significant cyber incident, as defined in PPD-41.

b. Coordinates with the USD(P) to integrate appropriate intelligence and intelligence-related activities as part of the whole-of-government effort supporting the cyber incident response.

c. Coordinates with the USD(P) on the planning and provision of cyber incident response support to mission partners.

9. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE. Under the authority, direction, and control of the USD(I) and in addition to the responsibilities in Paragraph 10, the Director, National Security Agency/Chief, Central Security Service notifies the ASD(HD&GS) when he or she receives a request for technical assistance from a non-DoD entity in response to a significant cyber incident, as defined in PPD-41.

10. DoD COMPONENT HEADS. The DoD Component heads:

a. Ensure that any DSCIR-related DoD issuances, concept plans, interagency agreements, and memorandums of understanding or agreement with external entities are in compliance with this DTM.

b. Ensure Component compliance with financial management guidance related to support provided for DSCIR operations, including guidance related to tracking costs and seeking reimbursement.

c. When approved by the Secretary of Defense, plan, program, and budget for DSCIR capabilities in accordance with law, policy, and assigned missions.

11. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in Paragraph 10 of this attachment, the Secretaries of the Military Departments:

a. Establish the necessary policies and procedures to ensure that appropriate personnel are trained to execute DSCIR plans, as directed by the Secretary of Defense.

b. Ensure that, when reimbursement of actual DSCIR expenditures is required, requests for reimbursement are made within 30 calendar days after the month in which performance occurred. Final billing invoices must be submitted to supported departments and agencies within 90 calendar days of the termination of the supported event.

12. CJCS. In addition to the responsibilities in Paragraph 10 of this attachment, the CJCS:

a. Advises the Secretary of Defense on the effects that supporting requests for DSCIR have on national security and military readiness.

b. Identifies available resources for support in response to DSCIR requests, and releases related orders when approved by the Secretary of Defense.

c. Notifies the Secretary of Defense when a DoD official provides DSCIR pursuant to immediate response authority. Notification should occur as soon as possible, but no later than 72 hours after the start of these DSCIR activities, and will include:

(1) Any action taken by a DoD official in support of a lead federal department or agency in response to the threat of or an actual cyber incident.

(2) The risk the threat or cyber incident presents to U.S. forces.

(3) The U.S. military personnel or material resources involved or expected to be involved in providing DSCIR.

(4) The expected duration of the DSCIR activity.

(5) Other pertinent threat or cyber incident-related information applicable to U.S. Government entities.

(6) Impacts on readiness.

d. Develops and maintains orders and instructions necessary for the execution of DSCIR. Such documents should include:

(1) Designations of supported and supporting relationships during support to cyber incident response.

(2) Categories of forces and capabilities for possible use in a cyber incident response.

(3) Command and control of forces supporting cyber incident response efforts.

e. Incorporates DSCIR into joint training and exercise programs in consultation with the USD(P&R); the Chief, National Guard Bureau (NGB); relevant Combatant Commanders; Commander, United States Cyber Command; and appropriate officials from the Department of Homeland Security and other federal departments and agencies.

f. Advocates for needed DSCIR capabilities that may be used to provide DSCIR and requirements through the Joint Requirements Oversight Council, subject to Paragraph 10.c. of this attachment, and the planning, programming, budgeting, and execution process.

13. COMMANDERS, UNITED STATES STRATEGIC COMMAND, UNITED STATES NORTHERN COMMAND, AND UNITED STATES PACIFIC COMMAND. In addition to the responsibilities in Paragraph 10 of this attachment, the Commanders of the United States Strategic, United States Northern, and United States Pacific Commands will carry out the following (the Commander, United States Strategic Command, will do so through United States Cyber Command):

a. In coordination with the CJCS and the combatant commanders, plan and execute DSCIR operations in accordance with this DTM, the Unified Command Plan, and the Global Force Management Implementation Guidance.

b. In coordination with the CJCS, incorporate DSCIR into joint training and exercise programs in consultation with the Department of Homeland Security, the Department of Justice, other appropriate federal departments and agencies, and the NGB.

c. When designated as supported commander, coordinate with supporting DoD Components all reimbursement for assistance provided under the provisions of this issuance.

d. When designated as supported commander, coordinate with the CJCS, the ASD(HD&GS), and any designated supporting commands for all military preparations and operations in support of lead federal departments and agencies during a cyber incident.

e. Inform the Secretary of Defense, through the CJCS and by the most expeditious means possible, of any actions taken to provide immediate response to save lives, prevent human suffering, or mitigate great property damage.

f. Provide situation and after-action reports for all DSCIR activities.

g. Advocate for capabilities that may be used to provide DSCIR and requirements through the Joint Requirements Oversight Counsel, subject to Paragraph 10.c. of this attachment, and the planning, programming, budgeting, and execution process.

h. Work closely with subordinate commands to ensure that they are appropriately reimbursed for DSCIR in accordance with Paragraph 10.b. of this attachment.

i. Exercise Training Readiness Oversight over assigned Reserve Component forces when not on active duty or when on active duty for training in accordance with DoDI 1215.06.

14. CHIEF, NGB. Under the authority, direction, and control of the Secretary of Defense, normally through the Secretary of the Army and the Secretary of the Air Force, and in addition to the responsibilities in Paragraph 10 of this attachment, the Chief NGB:

a. Serves as the channel of communications for all matters pertaining to the National Guard between DoD Components and the States, in accordance with DoDD 5105.77.

b. Annually assesses the readiness of the National Guard of the States to conduct DSCIR activities and reports on this assessment to the Secretaries of the Army and Air Force; the USD(P&R), ASD(HD&GS), and Assistant Secretary of Defense for Manpower and Reserve Affairs; and, through the CJCS, to the Secretary of Defense and appropriate combatant commanders.

c. Reports National Guard support of civil authorities or qualifying entities when using federal resources, equipment, and funding to the National Joint Operations and Intelligence Center, including DoD networks, software, and hardware.

d. Serves as an advisor to the combatant commanders on National Guard matters pertaining to their combatant command missions. Supports planning and coordination for DSCIR activities as requested by the CJCS or the combatant commanders.

e. Ensures that National Guard appropriations are appropriately reimbursed for DSCIR activities in accordance with Paragraph 10.b. of this attachment.

f. Advocates for capabilities that also may be used to provide DSCIR.

g. Develops and distributes, in accordance with DoDD 5105.77 and in coordination with the Secretaries of the Army and Air Force and the ASD(HD&GS), guidance regarding this DTM as it relates to National Guard matters.

ATTACHMENT 3

PROCEDURES

1. REQUESTS FOR DSCIR.

a. All requests for DSCIR will be submitted in writing to the DoD Executive Secretary. In emergency circumstances, requests for DSCIR may be oral. Oral requests that are approved must be followed by a written request at the earliest available opportunity.

b. All requests will include:

(1) A description of the specific assistance required, expressed in terms of desired outcome.

(2) The expected duration of the required assistance.

(3) A commitment to reimburse DoD, or a request for non-reimbursable support when reimbursement is not required by law, or when reimbursement may be waived by the Secretary of Defense in accordance with law and DoDD 3025.18.

c. All requests for DSCIR will be evaluated based on the criteria set in DoDD 3025.18, as well as the additional considerations identified in the policy section of this DTM.

2. IMMEDIATE RESPONSE AUTHORITY. Federal military commanders, DoD Component heads, and responsible DoD civilians may accept federal requests for DSCIR under immediate response authority in support of a cyber incident response according to the procedures provided in DoDD 3025.18, as well as the policy section of this DTM.

3. INFORMATION PROTECTION, RETENTION, AND SHARING.

a. DoD personnel will protect personally identifiable information in accordance with the Privacy Act of 1974 as implemented by DoDD 5400.11.

b. Authorization for disclosure and handling of classified, controlled unclassified information, unclassified information, personally identifiable information, and data shared with mission partners will be determined in accordance with U.S. law and DoD policies and guidance in accordance with Executive Order 12333; Executive Order 13526; title 32, Code of Federal Regulations, Part 2001; National Security Directive-42; National Disclosure Policy No. 1; DoDD 5230.11; DoDI 5200.01; and Volumes 3 and 4 of DoD Manual 5200.01.

c. Information that is incidentally acquired during the provision of DSCIR will be retained, disseminated, and disposed of in accordance with all applicable U.S. law and U.S. Government directives.

d. Information regarding threats or cyber incidents should be shared with other mission partners, as appropriate and in consultation with the federal department or agency receiving DSCIR.

e. Information acquired by DoD in the course of providing DSCIR will be treated as proprietary information and handled in accordance with DoD 5400.7-R.

4. REIMBURSEMENT. Policies and procedures for reimbursing DoD can be found in Volume 11A, Chapter 3 of DoD 7000.14-R.

## GLOSSARY

### PART I. ABBREVIATIONS AND ACRONYMS

ASD(HD&GS)	Assistant Secretary of Defense for Homeland Defense and Global Security
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
DoDD	DoD directive
DoDI	DoD instruction
DSCIR	Defense Support to Cyber Incident Response
NGB	National Guard Bureau
PPD	Presidential Policy Directive
U.S.C.	United States Code
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

### PART II. DEFINITIONS

asset response. Defined in PPD-41.

civil authorities. Defined in the DoD Dictionary of Military and Associated Terms.

cyber incident. Defined in PPD-41.

defensive cyberspace operations-response actions. Defined in the DoD Dictionary of Military and Associated Terms.

mission partners. For the purpose of this issuance, those with which DoD cooperates to respond to domestic emergencies such as other departments and agencies of the U.S. Government and, as appropriate, State, local, tribal, and territorial governments; multinational organizations; non-governmental organizations; and the private sector.

responsible DoD civilian. Defined in DoDD 3025.18.

offensive cyberspace operations. Defined in the DoD Dictionary of Military and Associated Terms.

threat. Defined in National Institute of Standards and Technology Interagency Report 7298, Revision 2.

threat response. Defined in PPD-41.

significant cyber incident. Defined in PPD-41.