DEFENSE HEALTH AGENCY
7700 ARLINGTON BOULEVARD, SUITE 5101 FALLS
CHURCH, VIRGINIA 22042-5101

DHA-IPM 18-015
January 28, 2020

MEMORANDUM FOR ASSISTANT SECRETARY OF THE ARMY (MANPOWER AND RESERVE AFFAIRS)
ASSISTANT SECRETARY OF THE NAVY (MANPOWER AND RESERVE AFFAIRS)
ASSISTANT SECRETARY OF THE AIR FORCE (MANPOWER AND RESERVE AFFAIRS)
DEPUTY ASSISTANT SECRETARY OF DEFENSE (HEALTH READINESS POLICY AND OVERSIGHT)
DEPUTY ASSISTANT SECRETARY OF DEFENSE (HEALTH SERVICES POLICY AND OVERSIGHT)
DEPUTY ASSISTANT SECRETARY OF DEFENSE (HEALTH RESOURCES MANAGEMENT AND POLICY)

SUBJECT: Interim Procedures Memorandum 18-015, Cybersecurity Program Management

References: See Attachment 1.

Purpose. This Defense Health Agency-Interim Procedures Memorandum (DHA-IPM), based on the authority of References (a) through (c), and in accordance with the requirements of References (d) through (y):

- Establishes the Defense Health Agency's (DHA) procedures to implement and maintain a DHA Cybersecurity Program for the Military Health System (MHS) to protect and defend DHA information and information technology (IT).

- Is effective immediately; it will be converted into DHA-Procedural Instruction (DHA-PI), "Cybersecurity Program Management." This DHA-IPM will expire effective 12 months from the date of issue.

Applicability. This DHA-IPM applies to Office of the Secretary of Defense, 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 (DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this DHA-IPM as the "DoD Components").

Policy Implementation. It is DHA's instruction, pursuant to References (d) through (y), to:

- Establish and maintain a DHA Cybersecurity Program in order to ensure that all IT under the authority, direction, and control of the DHA complies with DoD cybersecurity policy in accordance with References (d) through (y).

- Ensure that all IT under the authority, direction, and/or control of the Director, DHA, will be assigned to, and governed by, the DHA Cybersecurity Program that manages risk commensurate with the importance of supported MHS missions and the value of potentially affected information or assets.

- Operate secure and reliable networks and systems to protect computers, networks, programs, and data from unauthorized access or attacks.

- Focus on reception, reporting, and support for IT cybersecurity shared services already being provided.

- Monitor DHA IT user's behaviors to detect potentially unauthorized activity; and punitive methods and procedures will be applied in cases where uniformed, civilian, or contractor personnel are found in violation of applicable cybersecurity laws, policies, and/or standards. Failure to observe the prohibitions and mandatory provisions of this DHA-IPM by military personnel is a violation of the Uniform Code of Military Justice (UCMJ), Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel will be handled according to local laws and the terms of the contract. Additionally, violations by National Guard military personnel may subject members to prosecution under their respective State Military Code, or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.

Responsibilities. See Attachment 2.

Releasability. **Cleared for public release**. This DHA-IPM is available on the Internet from the Health.mil site at: www.health.mil/DHAPublications.

RONALD J. PLACE
LTG, MC, USA
Director

Attachments:
As stated

cc:
Principal Deputy Assistant Secretary of Defense (Health Affairs)
Surgeon General of the Army
Surgeon General of the Navy
Surgeon General of the Air Force
Medical Officer of the Marine Corps
Joint Staff Surgeon
Director of Health, Safety, and Work-Life, U.S. Coast Guard
Surgeon General of the National Guard Bureau
Director, National Capital Region

ATTACHMENT 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013, as amended
(b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013
(c) DHA-Procedural Instruction 5025.01, "Publication System," August 24, 2018, as amended
(d) Public Law 114-328, "National Defense Authorization Act for Fiscal Year 2017," December 23, 2016
(e) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended
(f) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(g) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015, as amended
(h) "DoD Cybersecurity Discipline Implementation Plan," October 2015, as amended
(i) Office of the Secretary of Defense Memorandum, "Department of Defense Cybersecurity Culture and Compliance Initiative," September 30, 2015[1]
(j) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended
(k) DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015, as amended
(l) DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, as amended
(m) DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)," March 21, 2014, as amended
(n) DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017
(o) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended
(p) DoD Directive 5500.07, "Standards of Conduct," November 29, 2007
(q) DoD 5500.7-R, "Joint Ethics Regulation," August 30, 1993, as amended
(r) DoD Chief Information Officer Memorandum, "Cybersecurity Scorecard Guidance," November 6, 2015[2]
(s) DoD Instruction 1400.25, Volume 731, "DoD Civilian Personnel Management System: Suitability and Fitness Adjudication For Civilian Employees," August 24, 2012

[1] This reference can be found at https://www.defense.gov.

[2] This reference can be found at https://dodcio.sp.pentagon.mil/sites/Collaboration/CSScorecard/_layouts/15/start.aspx#/Scorecard/Forms/AllItems.aspx (restricted access).

(t) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011
(u) DoD Instruction 8530.1, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016
(v) Joint Publication 3-12, "Cyberspace Operations," February 5, 2013
(w) DHA-Procedural Instruction 8140.01, "Acceptable Use of Defense Health Agency Information Technology (IT)," August 14, 2018, as amended
(x) DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015
(y) DHA-Interim Procedures Memorandum 18-013, "Risk Management Framework (RMF)," October 10, 2018

ATTACHMENT 2

RESPONSIBILITIES

1. DIRECTOR, DHA. Under the authority, direction, and control of the Assistant Secretary of Defense for Health Affairs, the Director, DHA, will:

a. Exercise management responsibility for Enterprise Activity functions in the MHS, including DHA Deputy Assistant Director, Information Operations/J-6 (DHA DAD IN/J-6) Cybersecurity Services, and develop appropriate management models for particular functions and processes.

b. Ensure compliance with References (d) through (y).

c. Report monthly inputs for the Secretary of Defense Cybersecurity Scorecard via DoD Cyberscope on the Secret Internet Protocol Router Network (SIPRNet) Defense Collaboration Services (https://emass-ers.csd.disa.smil.mil) per Reference (r).

d. Ensure individual and organization accountability within organizations under DHA's purview, including:

(1) Holding military medical treatment facility (MTF) Directors, Commanders, Authorizing Official (AO), Designated Representatives, Information System (IS) Owners, IS Security Managers, IS Security Officers, Program Managers (PMs), project and application leads, supervisors, and system administrators responsible and accountable for the implementation of DoD security requirements in accordance with this DHA-IPM and Reference (f).

(2) Ensuring that military and civilian personnel are considered for administrative or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place DoD information at risk by not ensuring implementation of DHA security requirements in accordance with this DHA-IPM, References (d) through (y), and supplemental DHA policies and procedures per Reference (f). Employ sanctions against individuals or units in accordance with the severity of non-compliance with cybersecurity policies, directives, and orders.

(3) Fundamentally shift cybersecurity cultural norms from the most senior leaders down to the unit and individual level, consistent with Reference (i). To treat access to DoD networks with the highest standards of individual knowledge, accountability, and reliability, that network access must be dependent on deliberate, disciplined, and effects-focused cyber behavior.

2. DHA CHIEF INFORMATION OFFICER (CIO). The DHA CIO will:

a. Develop, implement, maintain, and enforce a DHA Cybersecurity Program that is consistent with the strategy and direction of the DoD Senior Information Security Officer (SISO) and the Defense Cybersecurity Program, in accordance with Reference (f).

b. Ensure that IT under DHA's purview complies with References (d) through (y).

c. Ensure that cybersecurity requirements are addressed and visible in all capability portfolios, IT life-cycle management processes, and investment programs incorporating IT.

d. Ensure that Platform IT systems are identified, designated as such, and centrally registered.

e. Ensure that System Security Engineering and trusted systems and networks processes, tools, and techniques are used in the acquisition of all applicable IT under his/her purview per Reference (f).

f. Ensure that all personnel with access to DHA IT are appropriately cleared and qualified under the provisions of References (f), (m), and (n), and that access to all DoD IT processing specified types of information (e.g., collateral, Sensitive Compartmented Information, Controlled Unclassified Information) under his/her purview is authorized per References (f) and (j).

g. Ensure that personnel occupying cybersecurity positions:

(1) Are assigned in writing.

(2) Are trained and qualified in accordance with References (k) and (l).

(3) Are assigned a position designation using the criteria found in References (m) and (s), and consistent with DHA Mission Assurance publication. The position designation will be documented in the Defense Civilian Personnel Data System.

(4) Meet the associated suitability and fitness requirements.

h. Ensure that appropriate notice of privacy rights and monitoring policies are provided to all individuals accessing DHA-owned or controlled ISs.

i. Ensure that all ISs under DHA's purview are registered in the DoD IT Portfolio Repository at https://ditpr.dod.mil or the SIPRNet IT Registry at http://dodcio.osd.smil.mil/itregistry in accordance with current DoD IT Portfolio Repository and SIPRNet IT Registry guidance, or with the DoD Component Security Assistance Policy Coordinating Office for Security Assistance Policy ISs.

j. Ensure that all IT under DHA's purview complies with the applicable Security Technical Implementation Guide, Security Configuration Guides, and the Security Requirement Guide with any exceptions documented and approved by the responsible AO.

k. Report to the Director, DHA, on implementation of DoD/DHA security requirements and to whether military and civilian personnel knowingly, willfully, or negligently compromise, damage, or place DoD information at risk by not ensuring implementation of DoD/DHA security requirements in accordance with this DHA-IPM and other related DHA-PIs.

l. Designate an office responsible for coordinating identity authentication activities across the MHS.

m. Represent MHS interests in DoD/Veterans Affairs interagency efforts to standardize healthcare privacy and security requirements.

n. Ensure that all users understand and follow policy and guidance to protect classified and Controlled Unclassified Information, and prevent unauthorized disclosures on DoD IT in support of the DHA Mission Assurance Branch.

3. DHA SISO. The DHA SISO shall direct and coordinate the DHA Cybersecurity Program, applicable to all MTFs and Other Lines of Business (OLB) that are under the authority, direction, and control of the Director, DHA. The DHA SISO will:

a. Adhere to responsibilities listed in the DHA SISO appointment letter, posted to the Cyber Security Division (CSD) SharePoint site: https://info.health.mil/hit/infosec/SitePages/Home.aspx.

b. Implement and enforce the Risk Management Framework (RMF) within the DHA Cybersecurity Program consistent with Reference (e) and corresponding DHA-PIs.

c. Exercise management responsibilities for the DHA DAD IO/J-6 Cybersecurity Shared Service/Enterprise Activity functions in the MHS consistent with Reference (f) and cybersecurity shared services related to DHA-PIs.

d. Establish and oversee a team of Cyber Security professionals qualified in accordance with Reference (l), and supporting issuances, responsible for conducting security assessments.

e. Serve as Chair for the Cyber Security Work Group (CSWG). The CSWG Charter and additional information are posted to the CSD SharePoint site: https://info.health.mil/hit/infosec/SitePages/Home.aspx.

f. Implement and enforce DoD information network operations and defensive cyberspace operations internal defensive measures directed by DHA to protect the DoD information network within the DHA Cybersecurity Program consistent with References (t) through (y), and corresponding DHA-PIs and DHA-IPMs.

4. DHA AO. The DHA AO will be appointed by the Director, DHA, as AO for all DHA ISs and Platform IT systems under his/her purview, and ensure all DHA ISs and Platform IT systems are authorized in accordance with Reference (g). Responsibilities of the DHA AO are stipulated in the DHA AO Appointment Letter (posted to the CSD SharePoint site: https://info.health.mil/hit/infosec/SitePages/Home.aspx), References (e) and (f), and RMF related DHA-PIs.

5. REGIONAL INFORMATION OFFICERS AND DHA DEDICATED LIAISON OFFICERS. The regional information officers and DHA dedicated liaison officers will ensure the delivery of IT services for geographical regions via intermediary organizations as required, throughout the MHS, through clear communication, compliance, and utilization management.

6. MTF DIRECTORS AND OLB COMMANDING OFFICERS. MTFs will have one military officer who will be dual-hatted as the MTF Director, (under the authority, direction, and control of the Director, DHA), and the Service Commander, (under the authority, direction, and control of the Military Department concerned). Unless otherwise specified, and for the purpose of this DHA-IPM, the term "MTF Director" will be used to refer to dual-hatted position of the MTF Director and the Service Commander. The MTF Director and OLB Commanding Officers will:

a. Ensure Command/OLB cybersecurity staffing resources are adequate to cover applicable roles and responsibilities in this DHA-IPM and other DHA publications.

b. Ensure the designation, in writing, of a CIO and an Information System Security Manager (ISSM) to be responsible for the cybersecurity posture of the MTF/OLB, and the corresponding site Cyber Workforce PM to be responsible for coding and appropriate qualifications of all cybersecurity staff.

c. Fundamentally shift cybersecurity cultural norms from the most senior leaders down to the unit and individual level, consistent with Reference (i). To treat access to DoD networks with the highest standards of individual knowledge, accountability, and reliability, that network access must be dependent on deliberate, disciplined, and effects-focused cyber behavior.

d. Direct the provisions of Reference (i), in support of DoD's approach to cybersecurity.

e. Lead DHA change efforts and ensure adequate resourcing of capabilities and capacity that improve cybersecurity.

f. Be held accountable by the chain of command for the cybersecurity performance of their organization and the individuals who comprise it, and for the role cybersecurity performance plays in accomplishing assigned missions.

g. Set an example and help individuals master appropriate cyber behavior.

h. Ensure that appropriate action is taken against those who knowingly, willfully, or negligently compromise, damage, or place DoD information at risk by not ensuring implementation of DHA security requirements in accordance with this DHA-IPM. All available means, both administrative and judicial, may be taken, as appropriate.

i. Serve as the PM or ISO for the MTF/OLB enclave and performs duties in accordance with References (e) and (f), as well as DHA cybersecurity policy and guidance for system/applications within MTF operations.

7. MTF AND OLB CIOs. The MTF and OLB CIOs will:

a. Exercise authority, direction, and control over MTF and OLB IT/cybersecurity operations, respectively, and report to DHA DAD IN/J-6.

b. Support MTF Director/OLB Commanding Officer strategic and readiness priorities and ensure efficient operations through alignment with MHS enterprise DHA IT Cybersecurity Programs and policies.

c. Participate in DHA DAD IN/J-6 planning and information forums (e.g., Health IT Work Group, CSWG), to ensure DHA DAD IN/J-6 and cybersecurity staff understand what is important to them, and maintain working awareness of planned and in progress support efforts.

d. Communicate changes in and challenges with personnel, programs, cost, and contracts established in DHA DAD IN/J-6 baseline to DHA DAD IN/J-6. This includes notifying DHA DAD IN/J-6 of vacancies in cybersecurity positions that adversely impact effectiveness of cybersecurity operations.

e. Work with Command Human Resources to code all cybersecurity work roles in accordance with Reference (k). Perform or delegate responsibilities of the Command Cyber Work Force PM. Work with DHA DAD IN/J-6 Cyber Workforce PM and appropriate Regional Information Officer to ensure long term planning, costing, etc., of local cybersecurity staffing needs that satisfy the requisite knowledge, skills, abilities, and education requirements of cybersecurity staff consistent with Reference (k).

8. MTF AND OLB ISSMs. The MTF, and OLB ISSMs, is the primary cybersecurity technical advisor to the MTF Director (PM for the MTF enclave), AO, and ISO. For MTF enclaves, the ISSM manages the installation DHA Cybersecurity Program. The MTF and OLB ISSM may serve as the system ISSM for the enclave and reports to the MTF Director as the PM for the MTF enclave. Additionally, the MTF and OLB ISSMs will:

a. Adhere to responsibilities listed in References (e) and (f).

b. Adhere to responsibilities listed in DHA RMF and cybersecurity operations DHA-PIs.

c. Report to the MTF Director/Site Commander on all cybersecurity matters.

9. PMs. PMs assisted by supporting organizations to the acquisition community are responsible for the cybersecurity of their programs, systems, and information. This responsibility starts from the earliest exploratory phases of a program, with supporting technology maturation, through all phases of the acquisition. Acquisition activities include system concept trades, design, development, test and evaluation, production, fielding, sustainment, and disposal per Reference (g). The PM will:

a. Ensure cybersecurity is implemented in all system and service acquisitions at levels appropriate to the system characteristics and requirements throughout the entire life cycle of the acquisition, in accordance with Reference (f).

b. Ensure all acquisitions of qualifying IT have an adequate and appropriate cybersecurity strategy that will be reviewed prior to acquisition milestone decisions and acquisition contract awards in accordance with References (f) and (g).

c. Identify, implement, and ensure full integration of cybersecurity into all phases of the acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, operation, and sustainment in accordance with DHA guidance, Reference (e), and the DoD PMs Guidebook for Integrating the Cybersecurity RMF into the System Acquisition Lifecycle. The Guidebook can be accessed in the Defense Acquisition University Community of Practice:
https://www.dau.mil/cop/cybersecurity/Pages/Topics/Policies%20and%20Guidance.aspx.

d. Ensure the Program Management Office is resourced to support IS security engineering requirements and security technical assessments of the IT for the Security Control Assessor's recommendation, the AOs authorization decision, and other security-related assessments (e.g., Financial Improvement and Audit Readiness IT testing, Inspector General audits).

e. Ensure cybersecurity-related positions are assigned in accordance with established cybersecurity policy and guidance.

f. Appoint an ISSM, in accordance with Reference (e), for the program office and ensure the ISSM is certified in accordance with Reference (k).

g. Ensure the IT is registered in accordance with DHA and DoD portfolio management policy and guidance.

h. Develop and maintain a cybersecurity strategy for IT in accordance with DHA and DoD guidance.

i. Ensure applicable Cyber Tasking Orders are received and acted upon per the Cyber Tasking Orders directions accessible at the CSD SharePoint site: https://intelshare.intelink.gov/sites/dha-hit/CyOC/SitePages/CyOC%20Issuance.aspx.

j. Ensure test and evaluation of assigned ISs and IT systems are planned, resourced, and documented in the program test and evaluation master plan per Reference (g).

k. Ensure that the planning and execution of all RMF activities are aligned, integrated with, and supportive of the system acquisition process.

l. Ensure a Privacy Impact Assessment (PIA) (DD Form 2930) is completed for IT that collects, maintains, uses, and disseminates Personally Identifiable Information (PII) in accordance with Reference (o). Determine if the IT contains PII and establish necessary IT privacy requirements. For IT transitioning to the DHA that does not have a PIA, acquisition of new IT, or re-authorization of a current IT that did not previously have a PIA; complete a Privacy Threshold Analysis (PTA). The PTA can help the PM determine if the IT contains PII and establish related privacy requirements (e.g., PIA, system of records notice). A properly completed PTA provides documentation that the PM methodically considered privacy implications and whether a PIA is required. Upon completion of the PTA, e-mail the completed form to the DHA Privacy and Civil Liberties Office at: dha.ncr.pcl.mbx.piamail@mail.mil. PTA are to be competed via DHA Form 61.

m. Adhere to PM responsibilities listed in References (e) through (g), (x), (y) and corresponding DHA-PIs addressing RMF and cybersecurity operations.

10. AUTHORIZED AND PRIVILEGED USERS. Authorized and privileged users will adhere to all provisions stipulated in the corresponding System Access Authorization form in accordance with References (p), (q), and (w).

ATTACHMENT 3

PROCEDURES

MTF CIOs will, on behalf of MTF Directors/OLB Commanding Officers, determine whether they have adequate cybersecurity resources to fully staff and support Command cybersecurity operations at the site. Adequacy will be determined using the roles and responsibilities' requirements contained in this DHA-IPM, and the DHA DAD IN/J-6 staffing requirements commensurate with the size of the MTF. MTF CIOs will continue to monitor status of enterprise baseline and unique, local resources thereafter, and report status of all cybersecurity resources, including deficiencies, to DHA DAD IN/J-6 via appropriate channels (e.g., Chief Information Office Coordinating Committee, Health IT WG, CSWG).

The DHA SISO will ensure status, challenges, and progress of cybersecurity staffing are coordinated with all appropriate DHA DAD IN/J-6 and Program Management Office officials for appropriate action. Resources and actions to address cybersecurity requirements under the authority, control, and direction of the Director, DHA, will be balanced by each MTF Director's authority to prioritize tasks and resolve conflicts where necessary.

Each MTF Director/OLB Commanding Officer will leverage a designated DHA dedicated liaison officer to help identify and fill in gaps associated with MTF variance and immature/emerging cybersecurity processes, and for discussions with the DHA DAD IN/J-6 about tasking prioritization and conflict resolution.

The DHA SISO, DAD IO/J-6 CSD officials, MTF, and OLB cybersecurity officials will leverage the DHA DAD IN/J-6 CSD SharePoint site (https://info.health.mil/hit/infosec/SitePages/Home.aspx), for guidance on DHA's implementation of DoD policy, knowledge transfer, and collaboration.

GLOSSARY

ABBREVIATIONS AND ACRONYMS

AO	Authorizing Official
CIO	Chief Information Officer
CSD	Cyber Security Division
CSWG	Cyber Security Work Group
DAD IO	Deputy Assistant Director, Information Operations
DHA	Defense Health Agency
DHA-IPM	Defense Health Agency-Interim Procedures Memorandum
DHA-PI	Defense Health Agency-Procedural Instruction
DoD	Department of Defense
IS	information system
ISSM	Information System Security Manager
IT	information technology
MHS	Military Health System
MTF	military medical treatment facility
OLB	other lines of business
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PM	Program Manager
PTA	Privacy Threshold Analysis
RMF	Risk Management Framework
SIPRNet	Secret Internet Protocol Router Network
SISO	Senior Information Security Officer