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

DHA-IPM 18-013
September 20, 2019

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 18-013, Risk Management Framework (RMF)

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 guidance of References (d) through (ac):

- Incorporates cybersecurity strategy, policy, awareness/training, assessment, continuous monitoring, authorization, implementation, and remediation.

- Aligns with the Deputy Assistant Director, Information Operations (DAD IO) J-6/Chief Information Officer's (CIO) key concept of increasing cybersecurity of Defense Health Agency's (DHA) Information Technology (IT); therefore, robust risk assessment and management is required.

- Encompasses lifecycle risk management to determine and manage the residual cybersecurity risk.

- This DHA-IPM is effective immediately; it will be converted into a DHA-Procedural Instruction. This DHA-IPM will expire effective 12 months from the date of issue.

Applicability. This DHA-IPM 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 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").

- All military, civilian, and contract employees (when required by the terms of the applicable contract), and other individuals or organizations as required by binding agreement or obligation with the DHA, who develop, acquire, deliver, use, operate, support, or manage DHA IT.

- All networked or standalone IT used to receive, process, store, display, or transmit DHA information (or government information where the DHA agreed to manage the information/infrastructure), as well as DoD partnered systems where it is agreed that DoD standards are followed. DHA IT includes, but is not limited to: Information Systems (ISs) (major applications and enclaves), Platform Information Technology (PIT) (systems, subsystems, and products), IT services (internal and external), and IT products (software, hardware, and applications).

- Non-DoD ISs with DoD information that does not interface with DoD ISs (see Reference (t)).

- This DHA-IPM does not apply to the protection of Sensitive Compartmented ISs or intelligence, surveillance, reconnaissance mission, and mission support systems or higher authoritative guidance governing Special Access Program (SAP) systems.

Policy Implementation. It is DHA's instruction, pursuant to References (d) through (r), that this RMF:

- Provides a disciplined and structured process to perform DHA IT security and risk management activities and integrates those activities into the system development life cycle.

- Changes the traditional focus of certification and accreditation as a static, procedural activity to a more dynamic approach to more effectively manage mission and cybersecurity risks in diverse environments of complex, evolving, and sophisticated cyber threats and vulnerabilities.

- Ensures that DHA IT assets are assessed for cybersecurity risk to the DHA, and that the discovered weaknesses are documented in a Plan of Action and Milestones (POA&M) to mitigate risk, and an DHA AO supported by the RMF team members accepts the risk to the DHA AO's Area of Responsibility (AOR), in accordance with References (o) and (p).

- Ensures DHA-specific assignment values, overlays, implementation guidance, and assessment procedures are found on the DHA RMF Portal at: https://info.health.mil/hit/infosec/assessor/rmfipt/SitePages/home.aspx. As supporting reference security control documents are updated, DHA's implementation of these updates will be coordinated through the Assessment and Authorization Configuration Control Board.

- Ensure systems are authorized in accordance with this DHA-IPM. The DHA AO is appointed in writing for all DHA ISs and PIT systems operating within or on behalf of the DHA in accordance with Reference (p).

- Operates only authorized ISs and PIT systems (i.e., those with a current Authorization to Operate (ATO)), ATO with conditions, or interim authorization to test.

- Complies with all authorization decisions, including denial of ATO, and enforces authorization termination dates.

- Ensures personnel engaged in or supporting the RMF are appropriately trained and possess professional certifications consistent with Reference (o), and supporting issuances.

- Ensures Information System Owners (ISOs) appoint user representatives for DHA IS and PIT systems under the DHA's purview.

- Ensures that contracts and other agreements include specific requirements in accordance with this DHA-IPM.

Responsibilities. See Attachment 2.

Procedures. See Attachment 3.

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

for R. C. BONO
VADM, MC, USN
Director

Attachments:
As stated

cc:
Principal Deputy Assistant Secretary of Defense for 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 21, 2015, as amended
(d) Public Law 114-328, "National Defense Authorization Act for Fiscal Year 2017"
(e) Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014, as amended
(f) Committee on National Security Systems Instruction 1254, "Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems," August 31, 2016
(g) Committee on National Security Systems Instruction 4009, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015
(h) National Institute of Standards and Technology Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments," September 2012, as amended
(i) 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
(j) National Institute of Standards and Technology Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," January 22, 2015, as amended
(k) National Institute of Standards and Technology Special Publication 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," December 18, 2014, as amended
(l) National Institute of Standards and Technology Special Publication 800-60, Volume 1, Revision 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008
(m) National Institute of Standards and Technology Special Publication 800-60, Volume 2, Revision 1, "Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008
(n) National Institute of Standards and Technology Special Publication 800-82 Revision 2, "Guide to Industrial Control Systems (ICS) Security," May 2015
(o) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended
(p) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(q) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015, as amended
(r) Office of Management and Budget Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
(s) Secretary of Defense, "The Department of Defense Cyber Strategy," April 17, 2015
(t) DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012, as amended

(u) National Institute of Standards and Technology Special Publication 800-55, Revision 1, "Performance Measurement Guide for Information Security," July 2008
(v) DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," December 19, 2005, as amended
(w) DoD Directive 8140.01, "Cyberspace Workforce Management," July 31, 2017
(x) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended
(y) DoD Instruction 8551.01, "Ports, Protocols, and Services Management (PPSM)," May 28, 2014, as amended
(z) Committee on National Security Systems Instruction 4016, "National Information Assurance Training Standard for Risk Analyst," November 1, 2005
(aa) National Institute of Standards and Technology Special Publication 800-160, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," November 2016, as amended
(ab) DHA-Administrative Instruction 077, "Security Categorization (SC) and Control Selection for Information Technology (IT)," May 28, 2015
(ac) DHA-Administrative Instruction 042, "Security of Unclassified Department of Defense Information on Non-TRICARE Management Activity Information Systems," March 23, 2012

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. Appoint the DHA AO for the DHA Enclaves, ISs, and PIT systems in accordance with References (p) and (v).

b. Maintain the authority to revoke this appointment based on lack of diligence, non-compliance with responsibilities, and other security-related infractions.

c. Appoint the DHA IO pursuant to the requirements outlined in Reference (v), and the DHA Data Manager to assist the DHA IO with executing stated responsibilities.

2. DAD IO J-6/CIO. The DAD IO J-6/CIO will:

a. Provide guidance to organizations on how to implement solutions for operational requirements in support of established National, DoD, Joint Chiefs of Staff, or DHA security controls for IT and remain within established risk tolerance levels.

b. Ensure an ISO is appointed for all DHA IT.

c. Define cybersecurity performance measurements and metrics to identify enterprise-wide cybersecurity trends and status of mitigation efforts, in accordance with Reference (u).

d. Be responsible for the security controls implemented across the IT enterprise.

e. Ensure that an effective Information Security Continuous Monitoring (ISCM) program is established and implemented for the organization by establishing expectations and requirements for the organization's ISCM program.

f. Work closely with DHA AO to provide funding, personnel, and other resources to support ISCM.

g. Maintain high-level communications and working group relationships among organizational entities.

3. DHA SENIOR INFORMATION SECURITY OFFICER (SISO). The DHA SISO will:

a. Advocate for any budgets associated with duties below and advocate for DHA-wide

cybersecurity solutions through the planning, programming, budgeting and execution process on behalf of the DAD IO J-6/CIO.

b. Monitor, evaluate, and provide guidance to the DAD IO J-6/CIO regarding DHA cybersecurity posture.

c. Coordinate with the DAD IO J-6/CIO and DHA AO, to ensure the cybersecurity risk posture, risk tolerance levels, and risk acceptance decisions for DHA IT meet mission and business needs, while also minimizing the operations and maintenance burden on the organization.

d. Oversee establishment and enforcement of the DHA RMF, roles, and responsibilities; review approval thresholds and milestones within the RMF.

e. Participate in Federal, Joint, DoD, and DHA cybersecurity and RMF technical working groups and forums (e.g., Defense Security/Cybersecurity Authorization Working Group).

f. Adjudicate IT determinations, when a conflict in the IT determination process is identified.

g. Review and approve Privacy Impact Assessments (PIAs) submitted in accordance with Reference (x), and the Cyber Security Division PIA Workflow Process.

h. Establish, implement, and maintain the organization's ISCM program.

i. Develop organizational program guidance (i.e., policies/procedures) for continuous monitoring of the security program and ISs.

j. Develop configuration management guidance for the organization.

k. Provide training on the organization's ISCM program and process.

l. Provide support to DHA IOs/ISOs and common control providers on how to implement ISCM for their ISs.

4. DHA AO. The DHA AO is the official with the authority responsible for accepting a level of risk for a system balanced with mission requirements, except for IT with unmitigated "Very High" and "High" risk. The DHA AO is the only person with authority to grant authorization decisions within their AOR. The DHA AO will have the flexibility in augmenting, executing, and implementing RMF for systems in AOR. For example, the DHA AO can create a community-specific guidebook for better clarifying guidance. The DHA AO will:

a. Be appointed by Director, DHA. The appointment grants authority to authorize IT as defined in the DHA AO appointment memorandum.

b. Advocate for cybersecurity-related positions in accordance with References (o) and (p), and other cybersecurity related policy and guidance.

c. Ensure an ISO (i.e., the owner, operator, maintainer of the IT), is appointed prior to issuing an authorization decision.

d. Ensure ISOs participate throughout the RMF process and understand the risk imposed on the mission due to operating the IT.

e. Ensure verification through the DHA Ports, Protocols, and Services Office that Internet protocols, data services, and associated ports (internal and external), of the system/enclave comply with the requirements outlined in Reference (y).

f. Assist the DAD IO J-6/CIO in providing guidance to organizations on how to implement solutions for operational requirements exceeding the established National, DoD, Joint Chiefs of Staff, or DHA baseline controls for IT.

g. Render authorization decisions that balance mission needs with security concerns for IT within the DHA AO's AOR. The Authorization Decision Documentation will be digitally signed and generated via Enterprise Mission Assurance Support Service, except PIT. Any exceptions to or conditions of the authorization decision must be articulated within the Authorization Decision Document.

h. Review each system's Security Assessment Report (SAR), Risk Assessment Report, and POA&M to ensure there is a clearly defined course of action (also see Reference (h)). The DHA AO may downgrade or revoke an authorization decision at any time, if risk conditions or concerns so warrant.

i. Review and approve the security assessment plan, the security plan, and system-level ISCM strategy.

j. Ensure all DHA IT comply with DoD and DHA connection approval processes.

k. Not delegate authorization decision authority (i.e., to formally accept risk for a system).

l. Comply with DoD Information Security Risk Management direction issued on behalf of the Mission Area Principal AOs.

m. Consider how ISCM will be implemented organization-wide as one of the key components of the security life cycle represented by the RMF.

n. Approve the frequency of monitoring of the security controls based on the Integrated Strategy Model developed by the ISO or common control provider.

o. Review the reported security status of the system (including the effectiveness of security controls employed within and inherited by the system), on a continuous basis in accordance with

the ISCM strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.

p. Respond accordingly to the changed security status, which may include changing the authorization decision from an ATO to an ATO with conditions, or to a denial of ATO.

5. DHA AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE (AODR). The DHA AODR will:

a. Be appointed by the DHA AO. Appointments will be in writing (to include duties and responsibilities), to support the RMF. Digital signatures are authorized for appointment letters.

b. Complete and maintain required cybersecurity certification in accordance with Reference (v).

c. Perform responsibilities as assigned by the DHA AO. The DHA AODR may perform any and all duties of a DHA AO except for accepting risk by issuing an authorization decision.

d. Complete DHA AO training and maintain cybersecurity certifications consistent with duties and responsibilities of a DHA AO.

e. Provide recommendations to the DHA AO to render authorization decisions based on input from the DHA Security Control Assessor (SCA), ISO, Program Manager (PM), other DHA AO, and DHA AODRs.

f. Be supplemented with contractor support; however, contractors are not permitted to make decisions on behalf of the government and may only provide advice and guidance.

6. DHA SCA. The DHA SCA will:

a. Be appointed by the DHA SISO with the authority and responsibility for the assessment determination within their assigned AOR.

b. Complete and maintain required cybersecurity certification in accordance with Reference (v).

c. Evaluate the cybersecurity capabilities and services of a DoD IS and PIT system and make a recommendation for risk acceptance or denial to the DHA AO.

d. Review the SAP and ensure its integration into the program office's Test and Evaluation Master Plan (TEMP) in accordance with Reference (q).

e. Prepare the SAR documenting the issues, findings, and recommendations from the security control assessment, and reassess remediated controls, as required.

f. Review the authorization package, approve the SAR, and make an authorization recommendation to DHA AO.

g. Periodically assess security controls employed within and inherited by the IT in accordance with the ISCM program.

h. Determine the required further actions, once the DHA SCA is notified of the proposed system changes or actual changes to the environment of operations.

i. Provide input into the types of security-related information gathered as part of ISCM program and assesses IS or program management security controls for the organization's ISCM program.

j. Assess the security controls employed within and inherited by systems in accordance with the ISCM strategy.

k. Provide recommendations as to appropriate remediation actions.

l. Ensure appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate the identified risk.

m. Use the revised and updated artifacts to determine if a formal reauthorization action is necessary if there is a system or environment change.

7. DHA SECURITY CONTROL ASSESSOR REPRESENTATIVE (SCAR). The DHA SCAR may be an organic or contracted resource. The DHA SCAR works with the PM, Information System Security Manager (ISSM), Information System Security Officers (ISSOs), and Validators or Agent of the Security Controls Assessor (ASCA) to assess security controls for the DHA SCA. The DHA SCAR will:

a. Serve as an active member of the RMF team from its inception, to assist with planning of cybersecurity requirements.

b. Ensure security controls are implemented in accordance with the security plan and are assessed in accordance with the SAP.

c. Review the security assessment plan for each security control prior to conducting assessments.

d. Review the authorization package prior to submission to the DHA SCA.

8. DHA VALIDATORS. The DHA Validators will:

a. Develop the SAP and ensure its integration into the program office's TEMP in accordance with Reference (q).

b. Serve as an active member of the RMF team from its inception, to assist with planning of cybersecurity requirements. The DHA SCAR ensures security controls are implemented in accordance with the security plan and are assessed in accordance with the SAP.

c. Validate assessment results from others hands-on, comprehensive evaluations of the technical and non-technical security controls for the IT, determine the degree to which the IT satisfies the applicable security controls.

d. Review the authorization package prior to submission to the DHA SCAR.

9. ASCA. The ASCA is a licensed third-party agent assisting in assessment activities and providing an independent report for the SCAR and DHA SCA. This position cannot make decisions on behalf of the government but can only provide advice and guidance. The ASCA will:

a. Achieve and maintain an ASCA license per the DHA ASCA Guide.

b. Respond to PM, ISO, DHA SCAR, DHA SCA, and DHA AO requests for information regarding their respective systems.

c. Perform comprehensive evaluation of the technical and non-technical security controls for the IT, determine the degree to which the IT satisfies the applicable security controls, and provide mitigation recommendations.

d. Perform assessment procedures for each applicable security control as outlined in the DoD RMF Knowledge Service (KS) and DHA RMF Portal.

e. Review the authorization package prior to submission to the DHA SCAR.

f. Meet the intent of RMF independence between the PM or ISO and the individuals performing security control assessments; the ASCA reports their findings directly to the DHA SCA.

g. Not be part of the development team or program office. The PM or ISO provides funding for organizations or contractors to perform ASCA responsibilities; the PM or ISO does not provide direction or oversight to organizations or contractors in support of ASCA responsibilities.

h. Include safeguards to prevent a conflict of interests with the development team/PM to all ASCA agreements.

10. DHA IO. An organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, classification, collection, processing, dissemination, and disposal as defined in Reference (g). The DHA IO will:

a. Be appointed by the Director, DHA.

b. Provide input to the ISO regarding security requirements and security controls for the IT where the information is processed, stored, or transmitted.

c. Establish the rules for appropriate use and protection of the information, during generation, collection, processing, dissemination, and disposal; retain that responsibility even when the information is shared with or provided to other organizations.

d. Provide input to ISOs on the security controls selection (e.g., during system categorization and security controls tailoring), and on the derived security requirements for the systems where the information is processed, stored, or transmitted (a single IS, PIT system, or PIT subsystem may contain information from multiple IOs/stewards).

11. ISOs. Officials responsible for the overall procurement, development, integration, modification, and operation and maintenance of DHA IT. An ISO is appointed and performs all PM roles and responsibilities when a PM is not assigned. For DHA-wide systems, the ISO is appointed by the DHA Directorate responsible for the capability. The ISO will:

a. Identify the requirement for the IT and request funds to operate and maintain the IT in order to assure mission effectiveness.

b. Categorize the IT in accordance with Reference (e). ISO will use the information types as outlined in Reference (m).

c. Ensure, with coordination of the PM staff, the development, maintenance, and tracking of the security plan for assigned IT.

d. Ensure, with coordination of the PM staff, the development of an ISCM strategy to monitor the effectiveness of all security controls employed within or inherited by the system, and to monitor any proposed or actual changes to the system and its environment of operation.

e. Report the security status of the IT, including the effectiveness of security controls employed within and inherited by the system to the DHA AO and other appropriate organizational officials on an ongoing basis in accordance with the ISCM strategy.

f. Decide, in coordination with the DHA IO, who has access to the system (and what types of privileges or access rights) and ensure system users and support personnel receive the requisite security training.

g. Inform, based on guidance from the DHA SCA and DHA AO, appropriate organizational officials to conduct the Assessment and Authorization process or the Assess Only process; ensure the necessary resources are available for the effort, and provide the required IT access, information, and documentation to the DHA SCA.

h. Conduct the initial remediation actions on security controls based on the findings and recommendations on the SAR, and work with the DHA SCA and ISSM/ISSO to reassess remediated controls.

i. Ensure a POA&M is developed for all identified weaknesses, and the appropriate steps to mitigate those weaknesses are identified. Take appropriate steps to reduce or eliminate weaknesses, then generate the security authorization package and submit the package to the DHA SCA for assessment.

j. Ensure open POA&M items are updated and closed in a timely manner.

k. Ensure consolidated RMF documentation is maintained for systems with instances at multiple locations.

l. Thoroughly review the security controls assessment and risk assessment results before submitting the security authorization package to the DHA AO, ensuring the system's cybersecurity posture satisfactorily supports mission, business, and budgetary needs (i.e., indicates the mission risk is acceptable).

m. Ensure, with the assistance of the ISSM, and coordination with the PM staff, the system is deployed and operated according to the approved security plan and the authorization package (i.e., the DHA AO's authorization decision).

n. Initiate remediation actions on outstanding items listed in the POA&M and findings produced during the continuous monitoring of security controls.

o. Ensure security documentation, including the special publication and POA&M, is updated and maintained based on the results of the ISCM.

p. Be responsible for reporting the security status of the system.

q. Implement a system decommissioning strategy, as needed.

12. PM. The ISO is assigned the PM duties when no PM is assigned. The PM will:

a. Identify, implement, and ensure full integration of cybersecurity into all phases of the acquisition (ACQ), upgrade, or modification programs, including initial design, development, testing, fielding, operation, and sustainment in accordance with DHA guidance, and References (ab) and (ac).

b. Ensure the Program Management Office is resourced to support Information System Security Engineer (ISSE) requirements and security technical assessments of the IT for the DHA SCA's recommendation, the DHA AO's authorization decision, and other security-related assessments (e.g., Financial Improvement and Audit Readiness IT testing, Inspector General audits).

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

d. Appoint an ISSM, in accordance with Reference (ab), for the program office and ensure the ISSM is certified in accordance with Reference (v).

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

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

g. Ensure applicable Cyber Tasking Orders are received and acted upon per the Cyber Tasking Orders' directions.

h. Ensure Test and Evaluation of assigned IS and IT system is planned, resourced, and documented in the program TEMP per Reference (q).

i. Ensure the planning and execution of all RMF activities are aligned, integrated with, and supportive of the system ACQ process.

j. Ensure periodic reviews, testing, or assessment of assigned IT are conducted at least annually, and in accordance with the ISCM strategy.

k. Ensure operational systems maintain a current ATO and recommend to the DHA AO that systems without a current authorization are identified for removal from operation.

l. Ensure all system changes are approved through the DHA configuration management process, are assessed for cybersecurity impacts, and coordinated with the DHA SCA, DHA AO, and other affected parties, such as IOs and AOs of interconnected boundaries.

m. Track and implement the corrective actions identified in corresponding system POA&M in order to provide visibility and status to the ISO, DHA IO, DHA AO, and DHA SISO in a timely, recurring basis.

n. Report security incidents to stakeholder organizations and the DHA SCA. Conduct root cause analysis for incidents, and develop corrective action plans as input to the POA&M.

o. Ensure DD Form 2930, "Privacy Impact Assessment (PIA)" is completed for IT that collects, maintains, uses, and disseminates Personally Identifiable Information (PII) in

accordance with Reference (x), and DHA Privacy and Civil Liberties Office guidance at: https://info.health.mil/cos/admin/privacy/Privacy%20Compliance/SitePages/PrivacyCompliance.aspx). Determine if the IT contains PII and establish necessary IT privacy requirements. For IT transitioning to the DHA that does not have a PIA, ACQ of new IT, or re-authorization of a current IT that did not previously have a PIA; complete a DHA Form 61 "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, other). A properly completed PTA provides documentation that the PM methodically considered privacy implications and whether a PIA is required. Upon completion of the PTA Form, e-mail the PTA to the DHA Privacy Office at: dha.ncr.pcl.mbx.piamail@mail.mil.

p. Implement and assist the ISO in the maintenance and tracking of the security plan for assigned IS and PIT systems.

q. Enforce DHA AO authorization decisions for hosted or interconnected IS and PIT systems.

13. MEDICAL TREATMENT FACILITY (MTF) DIRECTORS AND OTHER LINES OF BUSINESS COMMANDING OFFICERS. MTF Directors and Other Lines of Business Commanding Officers will:

a. Serve as the PM or ISO for the MTF enclave and performs duties in accordance with Reference (o), and DHA cybersecurity policy and guidance for system/applications the MTF purchases.

b. Enforce DHA AO authorization decisions for hosted or interconnected IS and PIT systems.

14. ISSM. The ISSM is the primary cybersecurity technical advisor to the DHA AO, PM, and ISO. For MTF enclaves, the ISSM manages the installation cybersecurity program. The program ISSM may serve as the system ISSM for the enclave and reports to the MTF commander as the PM for the MTF enclave. The ISSM will:

a. Ensure the integration of cybersecurity into and throughout the lifecycle of the IT.

b. Complete and maintain required cybersecurity certification in accordance with Reference (v).

c. Ensure all DHA IT cybersecurity-related documentation is current and accessible to properly authorized individuals.

d. Support the PM or ISO in maintaining authorization to connect and authority to operate approvals and provide support to the PM or ISO in implementing corrective actions identified in the POA&M.

e. Coordinate, with the PM and DHA AO staffs, development of an ISCM strategy and monitor any proposed or actual changes to the system and its environment.

f. Continuously monitor the IT and environment for security-relevant events, assess proposed configuration changes for potential impact to the cybersecurity posture, and assess the quality of security controls implementation against performance indicators such as security incidents, feedback from external inspection agencies, exercises, and operational evaluations.

g. Ensure cybersecurity-related events or configuration changes that impact DHA IT authorization or adversely impact the security posture are formally reported to the DHA AO and other affected parties, such as IOs and AOs of interconnected IT.

h. Appoint ISSOs and provide oversight to ensure ISSOs follow established cybersecurity policies and procedures in accordance with Reference (p). (NOTE: ISSO appointments are not required).

i. Ensure all ISSOs and privileged users receive necessary technical training and obtain cybersecurity certification in accordance with Reference (w) and maintain proper clearances in accordance with Reference (p).

j. Ensure the DHA IT is acquired, documented, operated, used, maintained, and disposed of properly and in accordance with References (o) and (q).

k. Assist the DHA SCA in updating/maintaining the Risk Assessment Report and SAR based on the results of ISCM.

l. Assess the security controls employed within and inherited by systems in accordance with the ISCM strategy.

m. Provide recommendations as to appropriate remediation actions.

n. Provide the ISO and common control provider in an updated SAR, or another form (e.g., dashboard) in the interim for more critical security controls.

o. Ensure appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate the identified risk.

p. Be responsible for reporting the security status of the system to the DHA SCA and or DHA AO.

15. ISSO. The ISSO is responsible for ensuring the appropriate operational security posture is maintained for assigned IT. The ISSM will take on these responsibilities should no ISSO be assigned. This includes the following activities related to maintaining situational awareness and initiating actions to improve or restore cybersecurity posture. The ISSO will:

a. Implement and enforce all DoD and DHA cybersecurity policies, procedures, and countermeasures.

b. Complete and maintain required cybersecurity certification in accordance with Reference (v). Individuals in this position must be U.S. citizens, and the ISSO will ensure all users have requisite security clearances and need-to-know, complete annual cybersecurity training, and are aware of their responsibilities before being granted IT access.

c. Maintain all authorized user access control documentation in accordance with the applicable DHA Records Information Management System.

d. Ensure software, hardware, and firmware complies with appropriate security configuration guidelines (e.g., Security Technical Implementation Guides/Security Requirement Guides) can be found at: https://iase.disa.mil/stigs/Pages/index.aspx.

e. Ensure proper configuration management procedures are followed prior to implementation and contingent upon necessary approval.

f. Coordinate changes or modifications with the system-level ISSM, DHA SCA, and other designated personnel.

g. Initiate protective or corrective measures, in coordination with the security manager, when a security incident or vulnerability is discovered.

h. Report security incidents or vulnerabilities to the system-level ISSM and DHA cybersecurity office.

i. Initiate exceptions, deviations, or waivers to cybersecurity requirements.

j. Support the organization's ISCM program by assisting the ISO in completing ISCM responsibilities and by participating in the configuration management process.

k. Be responsible for reporting the security status of the system.

16. ISSE. The ISSE is an individual, group, or organization responsible for conducting ISSE activities and is required to be part of the ACQ process. ISSE captures and refines information security requirements and ensures the requirements are effectively integrated into IT products and ISs through purposeful security architecting, design, development, and configuration (see References (q) and (aa)), for additional details on systems engineering and IS engineering processes). The ISSE traces security controls (which are high-level cybersecurity capability needs), with the RMF team, to the actual system security requirements documented in the ACQ process (i.e., many security requirements are derived from security controls). The ISSE will:

a. Employ best practices when implementing security controls, including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques.

b. Coordinate their security-related activities with the ISSM, ISSO, ISO, and common control provider.

ATTACHMENT 3

PROCEDURES

1. RMF OVERVIEW. The 6-Step RMF process at RMF Tier 3 (system level) is based on the processes outlined in References (i) and (o). This process is iterative throughout the entire lifecycle for IT in accordance with References (q) and (ac).

a. Cybersecurity 6-Step RMF process and activities, as described in Reference (o), should be initiated as early as possible and fully integrated into the DoD ACQ process including requirements management, systems engineering, and test and evaluation. Integration of the RMF in ACQ processes reduces required effort to achieve ATO and subsequent management of security controls throughout the system life cycle (Reference (q)).

b. The DHA RMF Portal and the DoD RMF KS is the authoritative source for RMF implementation, planning, and execution. Where conflicts in guidance occur, the DoD RMF KS takes precedence.

c. This enclosure highlights the DHA-specific implementation, key DHA roles in each step, and additional resources required to complete the process. This DHA-IPM is intended to be a companion to the DoD implementation instructions. Specific implementation guidance is available on the DHA RMF Portal and DoD RMF KS.

2. RMF PROCESS

a. DHA RMF practitioners need ready access to RMF policy and guidance to effectively and efficiently apply the appropriate methods, standards, and practices required to protect DHA IT. Implementation guidance must reflect the most up-to-date DHA intent regarding evolving security objectives and risk conditions. To address this enterprise challenge, the DHA RMF Portal (https://info.health.mil/hit/infosec/assessor/rmfipt/SitePages/home.aspx) was established as the online, web-based resource that:

(1) Provides guidance and tools for implementing and executing DHA's implementation of RMF.

(2) Is the authoritative source for DHA RMF guidance and policies.

(3) Is available to those with IT risk management responsibilities for DHA IT.

(4) Supports automated/non-automated implementation of the DHA RMF process.

b. The DHA RMF Portal is accessible by individuals with a DoD Public Key Infrastructure certificate (Common Access Card).

(1) The DHA RMF Portal hosts a library of tools, diagrams, process maps, documents, etc., to support and aid in the execution of the DHA's implementation of the RMF.

(2) DHA Cyber Security Division is responsible for the functional configuration and content management of the Portal, and provides detailed analysis and authoring support for the Portal content.

(3) DHA ASCA Guide. The number and complexity of DHA IT may require the DHA SCA to designate qualified entities as ASCA to perform assessment actions. The DHA SCA created the DHA ASCA Guide to appoint licensed, qualified agents to provide accurate, consistent, and trusted DHA assessments.

3. RECIPROCITY AND REUSE. Cybersecurity reciprocity is an essential element in ensuring IT capabilities are developed and fielded rapidly and efficiently across the Military Health System Enterprise. Applied appropriately, reciprocity reduces redundant testing, assessing and documentation, and the associated costs in time and resources. The DoD RMF presumes acceptance of existing test and assessment results and authorization documentation.

When the acceptance of an existing security authorization is not feasible or appropriate, reuse is considered an acceptable alternative to reciprocity as described in Reference (o). Reuse is the leveraging of portions of a security authorization package documentation and results in order to reuse that information to support a new authorization. Reuse can represent significant resource savings to the leveraging organization, if full reciprocity is not possible. The DHA "Reciprocity and Reuse Guide" outlines the DHA RMF process for reciprocity and reuse under the security purview of the DHA and is published and maintained on the DHA RMF Portal.

GLOSSARY

ABBREVIATIONS AND ACRONYMS

ACQ	acquisition
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
AOR	Area of Responsibility
ASCA	Agent of the Security Controls Assessor
ATO	Authorization to Operate
CIO	Chief Information Officer
DAD IO	Deputy Assistant Director, Information Operations
DHA	Defense Health Agency
DHA-IPM	Defense Health Agency-Interim Procedures Memorandum
IO	Information Owner
IS	Information System
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
ISSE	Information System Security Engineer
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
KS	Knowledge Service
MTF	Medical Treatment Facility
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIT	Platform Information Technology
PM	Program Manager
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
RMF	Risk Management Framework
SAP	Special Access Program
SAR	Security Assessment Report
SCA	Security Control Assessor
SCAR	Security Control Assessor Representative

SISO	Senior Information Security Officer
TEMP	Test and Evaluation Master Plan