Think Privacy

Ensuring the appropriate security of personally identifiable information (PII) in IT is critical. PII is a piece of information contained within a document that constitutes a record. The time limit for PII retention depends on the type of record within which it is contained. Life-cycle management of Army records is governed by AR 25-400–2, The Army Records Information Management System (ARIMS).

The Privacy Act (PA) of 1974 provides protection (safeguards) for individuals against an invasion of privacy by federal agencies. The Army maintains records during the conduct of Army business. Army records, regardless of media, must be maintained from creation through final disposition in a manner that protects the rights and Interests of individuals and the Federal Government.

Definitions

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information.

PA record: Any item, collection, or grouping of information about an individual, regardless of physical form or characteristics, that (1) Is kept by the Government including an individual's home address, home telephone number, Social Security Number, education, financial transactions, medical history, and criminal or employment history; and (2) Contains an individual's name, identifying number, symbol, or other individual identifier such as a finger or voice print, or a photograph.

Privacy References

The Privacy Act (PA) of 1974, as amended
DoDI 5400.16, DoD Privacy Impact Assessment Guidance
AR 25-2, Army Information Assurance Program
AR 25-22, Army Privacy Program
AR 25-400-2, Army Records Information Management System (ARIMS)
AR 380-5, Army Information Security Program
DA Pam 25-403 Guide to Recordkeeping in the Army

Privacy Requirements For Systems

System owners must complete the following, and are invited to contact the TRADOC G-6 Records Management Office for assistance:

- Populate the Army Portfolio Management System (APMS) Records Management and Privacy Impact Assessment (PIA) tabs with complete, accurate information.
- Submit a Standard Form (SF) 115, Disposition of Federal Records to obtain authority for disposition of records. The National Archives and Records Administration (NARA) Archivist approves SF 115s and the U.S. Army Records Management and Declassification Agency publishes the dispositions in ARIMS.
- Complete a Department of Defense Form 2930, PIA for each existing TRADOC information system, application, or electronic collection (regardless of containing PA records or not).
- Complete a PA system of record notice (SORN) when PII is used to retrieve information from a system.
- Complete an Office of Management and Budget (OMB) Form 83-1, Paperwork Reduction Act (PRA) Submission and all required documentation when there is a collection of standardized data from ten of more members of the public (respondents) on an annual basis, unless such information collection falls under an exception to the PRA.
- Complete a PA statement whenever collecting information that will be maintained in a PA system of records (SOR), regardless of the medium used to collect the information.

This document is available for download at
http://www.tradoc.army.mil/Publications.asp
Users are invited to send suggested improvements to the Office of the TRADOC Deputy Chief of Staff, G-6,
usarmy.jble.tradoc.mbx.g-6-tradoc-iapm@mail.mil
Current as of: 23 FEB 17

System Owner's Guide to

Risk Management and Privacy

Ensuring Proper System Security

TRADOC G-6

RMF Overview

All Department of Defense (DoD) information technology (IT) that receive, process, store, display, or transmit DoD information must be assessed and approved IAW the Risk Management Framework (RMF). This applies to Stand-Alone Information Systems and Closed Restricted Networks as well as to IT connected to the DoDIN.

RMF BASIC STEPS

- Register in APMS and eMASS (naming conventions must be identical in both systems)
- Coordinate an SCA-V assessment at least six months prior to system expiration.
- Generate a POA&M.
- ATO approval/disapproval.
- Continuous Security Control Monitoring in eMASS

Register in eMASS

- Complete training at https://disa.deps.mil/ext/cop/iase/emass/Pages/training.aspx
- Complete a DD Form 2875, have it signed by your supervisor and security manager, and send it to TRADOC eMASS administrators at usarmy.jble.tradoc.mbx.g-6-tradoc-iapm@mail.mil
- Access eMASS to request an account.
  - NIPR https://emass-army.csd.dis.mil.
  - SIPR https://emass-army.csd.disa.mil.

  Be sure to click the verification link.
- Contact TRADOC eMASS administrators for assistance with registration. This will ensure the system is registered properly and you have a full understanding of the next steps.

SCA-V Request

- TRADOC G-6 will schedule SCA-V visits for all systems requiring reaccreditation
- For new systems, submit a bid request at https://army.deps.mil/NETCOM/sites/RMF/SitePages/Bid%20Tracker.aspx
- Coordinate with your resource manager and complete an Acquisition Management Oversight (AMO) packet. AMO packets typically require at least 3 quotes, although you can use the bid tracker as justification if you do not receive at least 3.

Self-Assessments

- Self-Assessments must be completed prior to any visit or assessment by the SCA-V team.
- They can take upwards of 45 days to complete if done properly.
- The Self-Assessment can be found within eMASS -> System Main -> Controls.
- Clicking a control will provide you a description, guidance, and references.
- When marking a control compliant or non-applicable, ensure your comments specifically reflect this. i.e. "Access Control is documented in our SOP 'TRADOC System Access Control Standard Operating Procedures' uploaded in the artifacts section."
- Your controls will be marked as "unofficial" until the SCA-V team conducts their final assessment.
- Once your final assessment is completed the SCA-V team will go in and mark them accordingly and as official.
- The first system you will need to inherit from is the "Army Policy Record." This will remove all the DoD-compliant controls for you.

Establish Inheritance

- Navigate to the system management tab -> inheritance then click Requests and Approvals.
- Find the system you will be inheriting from, click request, then save.
- Once approved, you will see the system on the System Summary tab within inheritance. Go here and select all the controls you will inherit.

POA&M /Final Steps

- To complete the POA&M process, you must add a vulnerability to all non-compliant controls: click on these controls and navigate to "Add AP vulnerability"
- Ensure all information is filled out correctly and is specifically addressing the vulnerability laid out by the SCA-V team.
- Once all non-compliant controls have been addressed and implementation plan filled out forward the package to the next step (Package tab—>Package status)
- At any stage the package can be pushed back for updates. Note you must respond within 5 business days.
- Upon final completion the AO will grant an ATO for up to 3 years at this point all POAM scheduled completion dates will be locked.

RMF References

DoDI 8500.01, Cybersecurity
DoDI 8510.01, Risk Management Framework for DoD Information Technology

Links

NETCOM Portal: https://army.deps.mil/NETCOM/sites/RMF/csdwiki/Home.aspx

RMF Knowledge Service: https://rmfks.osd.mil/login.htm