Ohio Military Reserve Regulation 25–22
Office Management

Privacy and Civil Liberties

Headquarters
Ohio Military Reserve
Haubrich Armory
4094 Sullivant Ave
Columbus, OH 43228

28 February 2024
29 March 2024

UNCLASSIFIED

SUMMARY

This new publication, dated 28 February 2024 —

- Sets forth the procedures and establishes the policies for ensuring the privacy and civil liberties of all Ohio Military Reserve (OHMR) personnel and anybody else whose Personally Identifiable Information (PII) is handled by the OHMR.
- Establishes the role and responsibilities of the OHMR Chief Privacy Officer (CPO).
- Defines PII, Sensitive PII (SPII), and non-sensitive PII as these terms pertain to the OHMR.

History. This publication is a new Ohio Military Reserve regulation.

Applicability. Unless otherwise stated, this regulation applies to all OHMR information system or service (ISS) users.

Proponent and exception authority. The proponent of this publication is the CPO, though the OHMR Commander may act as proponent without the consent of the CPO. The proponent has the authority to approve exceptions or waivers to this publication that are consistent with controlling law and regulations. The proponent may not delegate this approval authority. Activities may request a waiver to this publication by providing justification that includes a full analysis of the expected benefits and must include formal review by the OHMR Judge Advocate General (JAG). All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent.

Suggested improvements. Users are invited to send comments and suggested improvements directly to ohmrcpo@sdf.ohio.gov.

Distribution. This regulation is available in electronic media only and is intended for OHMR ISS users.

Chapter 1
Introduction

1–1. Purpose
This regulation sets policies and procedures for ensuring the privacy and civil liberties of all OHMR ISS users and anybody else whose PII is handled by the OHMR. It establishes the role of the OHMR CPO. It also defines PII, Sensitive PII (SPII), and non-sensitive PII as these terms pertain to the OHMR. This regulation enacts Ohio Revised Code (ORC) Section 1347.15 and the privacy controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5. Each privacy control derived from NIST SP 800-53 is referenced using privacy control citations placed in brackets ("[AC-3(14)]"). The privacy controls implemented in this regulation include those recommended in NIST SP 800-122. This regulation is required to comply with statute and policy realized through the implementation of NIST SP 800-53. This regulation uses federal privacy terminology to maximize the OHMR's interoperability with the Ohio National Guard even as it enacts ORC Section 1347.15(B).

1–2. References, forms, and explanation of abbreviations
See appendix A.

1–3. Associated publications
This section contains no entries.

1–4. Responsibilities
a. Ohio Military Reserve Chief Privacy Officer. The CPO will—
(1) Serve as the senior OHMR policy official for all organizational privacy and civil liberty concerns.
(2) Implement and adhere to Chapter 2 of this regulation.
(3) Ensure in accordance with (IAW) ORC Section 1347.15(H)(3) that no person who was ever convicted of or pleaded guilty to a violation of ORC Section 1347.15(H)(1) or (H)(2) is permitted entry into the OHMR.

b. Ohio Military Reserve Information System or Service Users. OHMR ISS users will–
(1) IAW ORC Section 1347.15(H)(1), never knowingly access another person's SPII in violation of an Ohio state agency's rule. A violation of ORC Section 1347.15(H)(1) is a misdemeanor of the first degree IAW ORC Section 1347.99.
(2) IAW ORC Section 1347.15(H)(2), never knowingly use or disclose confidential personal information in a manner prohibited by law. A violation of ORC Section 1347.15(H)(2) is a misdemeanor of the first degree IAW ORC Section 1347.99.
(3) Adhere to sections of this regulation directed at OHMR ISS users ("OHMR ISS users will…").
(4) Inquire with the CPO for privacy and legal counsel regarding any questions or concerns about this regulation or OHMR ISS user responsibilities.

1–5. Records management (recordkeeping) requirements
The records management requirement for all record numbers, associated forms, and reports required by this publication will be IAW ORC Section 149.43, and the regulations and policies of the Ohio Adjutant General's Office.

Chapter 2
Privacy Controls

2–1. Access Control
a. Individual Access [AC-3(14)]. The CPO will ensure OHMR ISS users are able to access any final (but not draft) document or record stored in an OHMR ISS which contains their PII, other than cybersecurity audit logs or any information used by the Ohio State Defense Force (OHSDF) or OHMR in an investigation.
b. Information Sharing [AC-21]. The CPO will ensure policies and procedures are made available to OHMR ISS users to describe how their PII stored in an OHMR ISS may be shared with other users IAW

ORC Section 1347.15(B)(1), (B)(2), and (B)(5). The CPO will require OHMR ISS users to acknowledge receipt of these policies and procedures IAW ORC Section 1347.15(D).

2–2. Awareness and Training

a. Policy and Procedures [AT-1]. The CPO will–

(1) Ensure the annual administration IAW ORC Section 1347.15(C)(2) of Identifying and Safeguarding Personally Identifiable Information (ISPII) training from the Defense Counterintelligence and Security Agency's Center for Development of Security Excellence for all OHMR ISS users.

(2) Apprise OHMR personnel of updates to Privacy and PII Protection, Processing, and Transparency (P4T) policy and/or procedures as they are approved.

b. Training Records [AT-4]. The CPO will ensure individual annual ISPII training records are documented, monitored, and retained indefinitely.

2–3. Incident Response

a. Training [IR-2(3)]. The CPO will ensure all OHMR ISS users are trained annually on how to identify and respond to an SPII breach and on the OHMR's process for responding to an SPII breach.

b. Incident Response Plan [IR-8(1)]. The CPO will ensure any OHMR incident response plan for any breach that involves SPII includes:

(1) A process for notifying all affected individuals and appropriate oversight organizations as appropriate and required by law, regulation, or policy IAW ORC Section 1347.15(B)(6).

(2) An assessment process for determining the extent of the harm, embarrassment, inconvenience, and/or unfairness to affected individuals and any mechanisms or remedies for mitigating harm.

(3) Identification of applicable privacy requirements.

2–4. Media Protection

a. Media Marking [MP-3]. OHMR ISS users will never store the SPII of any other OHSDF or OHMR personnel on any personally owned electronic device or digital media without their express prior written consent.

b. Media Sanitization [MP-6]. OHMR ISS users will–

(1) Sanitize any digital media that contains the SPII of other OHSDF or OHMR personnel IAW NIST SP 800-88 Revision 1 Section 5 prior to the digital media's disposal, release from organizational control, or release for reuse.

(2) Destroy any printed media that contains the SPII of OHSDF or OHMR personnel IAW CUI Notice 2019-03.

2–5. Privacy Program Plan

a. Measures of Performance [PM-6]. The CPO will develop, monitor, and report to the OHMR Commander on the performance of privacy measures.

b. Privacy Program Plan [PM-18]. The CPO will–

(1) Develop, approve, and disseminate to OHMR ISS users the OHMR privacy program plan that defines procedural privacy controls and manages the privacy risk to OHSDF and OHMR operations, mission, functions, image, reputation, organizational assets, personnel, partner organizations, and the State of Ohio.

(2) Review the OHMR privacy program plan at least annually and update it whenever required due to changes in federal or state privacy laws, policy, organizational changes or because of problems identified during plan implementation or privacy control assessments.

c. Privacy Program Leadership Role [PM-19]. The CPO will–

(1) Coordinate, develop, and implement applicable privacy requirements and manage privacy risks through the OHMR privacy program.

(2) Be seated on any Data Integrity Board (DIB) or Data Management Board (DMB) chartered by the OHMR.

(3) Either be the OHMR JAG or another individual in the OHMR who is formally named as the CPO by the OHMR Commander after nomination by the OHMR JAG.

d. Dissemination of Privacy Program Information [PM-20]. The CPO will ensure OHMR public websites–

(1) Describe the OHMR's privacy policies and program IAW ORC Section 1347.15(D).

(1) Enable the public to learn about OHMR privacy activities.

(2) Publicize OHMR privacy practices and reports.
(3) Provide ohmrcpo@sdf.ohio.gov as an email by which the public may ask questions or provide feedback on OHMR privacy practices.

e. Privacy Policies on Websites, Applications, and Digital Services [PM-20(1)]. The CPO will ensure OHMR privacy policies–

(1) Are posted on all OHMR public-facing websites.
(2) Are written in plain language and organized to be easy to understand and navigate.
(3) Provide information needed by the public to make an informed decision about whether and how to interact with the OHMR.
(4) Are updated whenever the OHMR makes a substantive change to the described practices.
(5) Include a time/date stamp to inform the public of the date of the most recent changes.
(6) Are linked on any known, major entry points to the OHMR website(s), as well as any webpage on which PII is handled.

f. Accounting of Disclosures [PM-21]. OHMR ISS users will–

(1) Ensure an accurate accounting of SPII disclosures to entities external to the OHSDF (including OHMR) is developed and maintained using any system that can accurately list all disclosures. The accounting will include disclosure date; the nature of the disclosure; the purpose of each disclosure; and the name and address (or other contact information) of the entity to whom the disclosure was made.
(2) Retain the accounting of SPII disclosures.
(3) Ensure the accounting of SPII disclosures is made available upon request to the individual(s) whose PII was disclosed so they can learn to whom their PII has been disclosed, to provide a basis for subsequently advising recipients of any corrected or disputed PII, and to provide an audit trail for subsequent reviews of OHMR compliance with conditions for disclosures.

g. Personally Identifiable Information Quality Management [PM-22]. The CPO will–

(1) Develop, document, and disseminate OHMR policies and procedures for the review of PII to ensure its accuracy, relevance, timeliness, and completeness; correction or deletion of inaccurate or outdated PII; dissemination of notices of corrected or deleted PII to individuals or other appropriate entities; and the appeal of adverse decisions on correction or deletion requests.
(2) Ensure that practical means and mechanisms exist and are accessible for individuals or their authorized representatives to seek the correction or deletion of PII.
(3) Ensure that processes for correcting or deleting data are clearly defined and made publicly available.
(4) Determine what PII is to be retained, deleted, and/or corrected based on the scope of requests, the changes sought, and the impact of the changes.
(5) Manage a process for providing responses to individuals of decisions to deny requests for correction or deletion that include the rationale for decisions, a means to record individual objections to decisions, and a means of requesting reviews of initial determinations
(6) Ensure individuals or their designated representatives are notified when their PII is corrected or deleted to provide transparency and confirm the action is completed.

h. Data Integrity Board [PM-24]. The OHMR will convene a DIB whenever the OHMR receives a proposal to conduct or participate in a computer matching program or to conduct a review of computer matching programs in which the OHMR has participated.

i. Minimization of Personally Identifiable Information Used in Testing, Training, and Research [PM-25]. The CPO will–

(1) Develop, document, implement, review annually, and update as necessary policies and procedures for minimizing the handling of PII by using placeholder (“dummy” or “bogus”) data whenever possible during OHMR ISS testing or training.
(2) Authorize the use of PII in ISS testing or training to ensure the handling of PII during ISS testing or training is minimized. This does not preclude the handling of PII in real-world OHMR operations, communications, or recordkeeping, which are a necessary part of official OHMR business.

j. Complaint Management [PM-26]. The CPO will implement a process for receiving and responding to complaints, concerns, or questions from individuals about OHMR privacy practices that provides–

(1) Mechanisms that are easy to use and readily accessible by the public.
(2) All information necessary for complaints to be successfully filed.
(3) Tracking mechanisms to ensure all complaints are reviewed and addressed within 30 days;

(4) Acknowledgement within seven days of receipt of complaints, concerns, or questions from individuals;
(5) Response to complaints, concerns, or questions from individuals within 14 days.
(6) The means by which PII is handled IAW this regulation.

k. Privacy Reporting [PM-27]. The CPO will disseminate OHMR privacy reports annually to both the Commanding General of the OHSDF and the OHMR Commander.

2–6. Privacy and Personally Identifiable Information Processing and Transparency (P4T)

a. Policy and Procedures [PT-1]. The CPO will–
(1) Develop, document, and disseminate a P4T policy to OHMR ISS users. The policy will address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
(2) Develop, document, and disseminate P4T procedures to facilitate OHMR's implementation of P4T policy and privacy controls.
(3) Review and update P4T training policies and procedures at least annually and whenever assessment or audit findings, breaches, changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines necessitate updates.

b. Authority to Process Personally Identifiable Information [PT-2]. The CPO will–
(1) Determine and document the laws, executive orders, directives, regulations, and/or policies that authorize the processing of PII by OHMR ISS users.
(2) Ensure all OHMR ISS users are trained in the laws, executive orders, directives, regulations, and/or policies that authorize OHMR ISS users to process PII. Processing includes (but is not limited to) creation, collection, use, logging, storage, maintenance, dissemination, disclosure, and disposal.
(3) Ensure all OHMR ISS users are instructed to consult with the CPO for privacy and legal counsel regarding the OHMR's authority to process PII.

c. Personally Identifiable Information Processing Purposes [PT-3].
(1) The CPO will–
(a) Identify, document, and describe in public privacy notices and policies the OHMR's purposes for processing PII.
(b) Ensure revisions of the OHMR's privacy policies are rapidly disseminated to all OHMR ISS users.
(2) OHMR ISS users will–
(a) Restrict the processing of PII only to that which is compatible with the OHMR's purposes for processing PII, as stated in the OHMR's public privacy notices and policies.
(b) Obtain renewed consent from all OHMR ISS users impacted by any changes in the processing of PII that result from revision of OHMR privacy policies.

d. Consent [PT-4]
(1) The CPO will–
(a) Approve the format of any OHMR form that is used to collect SPII before it is first used.
(2) OHMR ISS users will–
(a) Obtain individually agreed-upon consent from other OHSDF or OHMR personnel prior to collecting or processing their SPII using a written agreement that provides a mechanism by which an individual may revoke consent after it has been provided, uses plain language, and avoids technical jargon.
(b) Notify OHMR recruits that their failure to consent to the collection and processing of their SPII may result in their not being permitted to serve in the OHMR.

e. Privacy Notice [PT-5]. OHMR personnel will provide clear, easy-to-understand, plainly stated notice to individuals regarding the processing of their PII upon their first interaction with the OHMR and annually thereafter and identify both the authority authorizing the processing of PII and the purposes for which PII is to be processed.

f. Specific Categories of Personally Identifiable Information [PT-7]. The CPO will ensure privacy policies and ISPII training discuss specific categories of PII identified in laws, executive orders, directives, regulations, policies, standards, or guidelines for which special protections and processing conditions are required.

g. Social Security Numbers [PT-7(1)]. OHMR personnel will–

(1) Never unnecessarily collect, maintain, or use anybody else's Social Security Number (SSN).
(2) Use OH|ID numbers as their personal identifiers in lieu of SSN in all official OHMR business unless an OHSDF or OHMR form explicitly requires SSN entry.
(3) Never deny individuals their rights, benefits, or privileges provided by law because of their refusal to disclose their SSN.
(4) Inform any individual who is asked to disclose SSN whether disclosure of SSN is mandatory or voluntary, by what statutory or other authority such number is solicited, and what use(s) will be made of it.

h. First Amendment Information [PT-7(2)]. OHMR ISS users will never process information describing how any individual exercises rights guaranteed by the First Amendment of the United States Constitution unless processing is expressly authorized by statute, by the individual, or unless pertinent to and within the scope of an authorized law enforcement activity.

i. Computer Matching Requirements [PT-8]. The CPO will ensure the following items are accomplished by the OHMR as part of a computer matching program:

(1) Approval is obtained from the DIB before any PII is processed.
(2) A computer matching agreement is reached before any PII is processed.
(3) A computer matching notice is published before any PII is processed.
(4) The information produced by the computer matching program is independently verified before taking adverse action against an individual.
(5) Individuals are provided with notice and an opportunity to contest computer matching findings before adverse action is taken against them.

2–7. Risk Assessment

Privacy Impact Assessments (PIA) [RA-8]. The CPO will approve in advance any PIAs conducted by OHMR personnel and coordinate on any PIAs conducted by the Ohio Adjutant General's Office IAW ORC Section 1347.15(B)(8).

2–8. System and Services Acquisition

Security and Privacy Engineering Principle of Minimization [SA-8(33)]. OHMR ISS users will implement the privacy principle of minimization such that only SPII that is directly relevant and necessary to accomplish an authorized purpose is processed and that SPII is only maintained for as long as is necessary to accomplish the purpose.

2–9. System and Communications Protection

Boundary Protection [SC-7]. OHMR ISS users will only process PII IAW established privacy requirements and will limit PII processing by minimizing the sensitivity of data field entries in databases and forms (whether electronic or written and scanned).

2–10. System and Information Integrity

a. Information Management and Retention [SI-12]. OHMR ISS users will ensure records and other information that contain SPII are retained IAW applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

b. Limit Personally Identifiable Information Elements [SI-12(1)]. OHMR ISS users will limit the processing of SPII in OHMR ISSs to the minimum necessary to execute and sustain OHMR operations by minimizing the sensitivity of data field entries in databases and forms (whether electronic or written and scanned) and restricting the transmission of SPII in electronic correspondence.

c. *Minimize Personally Identifiable Information in Testing, Training, and Research* [SI-12(2)]. OHMR ISS users will–

(1) Receive formal advance approval from the CPO before the SPII of OHMR ISS users is used in research that involves the OHMR.
(2) Never use SPII in OHMR training publications or materials.

d. Information Disposal [SI-12(3)]. OHMR ISS users will delete personnel records and other SPII from OHMR ISSs at the earliest opportunity IAW applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

e. Personally Identifiable Information Quality Operations [SI-18]. OHMR ISS users will initiate correction(s) of their own erroneous PII in records or stored in OHMR ISSs by submitting OHMR Form

5914 upon their identification of inaccurate or outdated PII to ensure updates or corrections to PII are tracked over time in personnel records.

f. Individual Requests [SI-18(4)]. OHMR personnel will–

(1) Ensure erroneous PII is corrected upon the request of the individual whose PII is incorrect or the individual's designated representative.

(2) Delete an individual's PII upon the request of the individual or their designated representative to avoid circumstances in which the retention of PII causes problems for OHMR ISS users that outweigh the benefit to the OHMR of PII retention, except in cases defined by the CPO.

g. De-identification [SI-19]. OHMR ISS users will de-identify PII handled by OHMR ISSs at the discretion of the CPO or when handling of the PII is no longer necessary.

Appendix A
References

Section I
Required Publications

Controlled Unclassified Information (CUI) Notice 2019-03
Destroying CUI in paper form (cited in Section 2-4)

CUI Registry
Sensitive Personally Identifiable Information (cited in Section 2-1)

NIST SP 800-53 Revision 5
Security and Privacy Controls for Information Systems and Organizations (cited in Section 1-1)

NIST SP 800-88 Revision 1
Guidelines for Media Sanitization (cited in Section 2-4)

NIST SP 800-122
Guide to Protecting the Confidentiality of Personally Identifiable Information (cited in Section 1-1)

ORC Section 149.43
Availability of public records for inspection and copying (cited in Section 1-5)

ORC 1347.15
Access rules for confidential personal information (cited in Section 1-5)

OHMR Reg 25-1
Information Technology (cited in Section 2-2)

Section II
Prescribed Forms

OHMR Form 5914
Additions and Corrections to Personal Information Record (cited in Section 2-10)

Glossary

Section I
Abbreviations

ABCA
abbreviations, brevity codes, and acronyms

Section II
Terms

Acronym
A word formed from the initial letters of a name or parts of a series of words (for example, “OHMR” for Ohio Military Reserve or “SPII” for Sensitive Personally Identifiable Information).

Breach
The compromise, loss of control, unauthorized disclosure, or unauthorized acquisition of PII in which either 1) a person other than an authorized handler accesses or potentially accesses PII or 2) an

authorized handler accesses or potentially accesses such information for other than authorized purposes. Any incident that involves SPII is considered a breach.

Brevity code
A shortened form of frequently used phrases, sentences, or a group of sentences normally consisting entirely of upper-case letters (for example, IAW for In Accordance With).

Computer matching
A computerized comparison of records that contain PII from two or more databases stored in automated information systems of records or an automated system of records and automated records maintained by a federal or state agency. Computer matching programs involve not just the matching activity itself but also the investigative follow-up and any appropriate action.

De-identification
The general term for the process of removing the association between a set of identifying data and the data subject. Many datasets contain information about individuals that can be used to distinguish or trace an individual's identity, such as name, SSN, date and place of birth, mother's maiden name, or biometric records. Datasets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Removing identifiers improves privacy protection since information that is removed cannot be inadvertently disclosed or improperly used.

Non-sensitive personally identifiable information
An individual's full name, grade, rank, organization (OHSDF, OHMR, etc.), unit, normal duty location, official ohio.gov email address, telephone number (as provided by the individual), visual image (photograph or video) while the individual is in OHMR or other daily business attire, or OHMR ISS user account identification ("username"). Groupings of this information remain non-sensitive.

Chief Privacy Officer (CPO)
The senior OHMR official responsible for coordinating, developing, and implementing applicable privacy requirements and managing privacy risks through the OHMR privacy program. The CPO shall be seated on any OHMR DIB or DMB chartered by the OHMR. The CPO is either the OHMR JAG or a staff member of the OHMR JAG who is formally named to be the CPO by the OHMR Commander after being nominated by the OHMR JAG.

Ohio Military Reserve (OHMR) Information System or Service (ISS) User
Any person for whom an active, authorized individual user account issued by the OHMR-S6 section exists on an OHMR ISS. OHMR ISS users include all OHMR personnel and all personnel from the OHSDF Command Staff who are issued accounts by the OHMR-S6 section to use any OHMR ISS.

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

Privacy Program Plan
A formal document agreed upon by specific OHMR personnel that provides an overview of the OHMR's privacy program and includes a description of the structure of the privacy program; the resources dedicated to the privacy program; the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements; the role of the CPO and the identification and assignment of roles of other privacy officials and staff and their responsibilities; the strategic goals and objectives of the privacy program; a description of the leadership commitment, compliance, and the strategic goals and objectives of the privacy program; and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. The plan must provide sufficient information about the privacy program management and common controls to enable control implementations that are compliant with the intent of the plan and a determination of the risk incurred if the plan is implemented as intended.

Sensitive Personally Identifiable Information (SPII)

A subset of PII that could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual if lost, compromised, or disclosed. Some forms of PII are sensitive as stand-alone elements. Stand-alone SPII includes an individual's SSN, driver's license, or state identification number; alien registration number; financial account number; or biometric identifier (such as fingerprint, voiceprint, or iris scan). Any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements are SPII: truncated SSN (last four digits), date of birth, citizenship or immigration status, ethnic or religious affiliation, sexual orientation, criminal history, system authentication information (such as mother's maiden name, account passwords, or personal identification numbers), or military performance rating. OHMR personnel records are SPII once PII is present, whether a record is in draft or final form. SPII is defined in the CUI Registry and is functionally equivalent to the term "confidential personal information" defined in ORC Section 1347.15(A)(1).