



DEPARTMENT OF THE NAVY
COMMANDER
NAVAL EDUCATION AND TRAINING COMMAND
250 DALLAS STREET
PENSACOLA, FLORIDA 32508-5220

NETCINST 5211.2E
N00J
17 Oct 2024

NETC INSTRUCTION 5211.2E

From: Commander, Naval Education and Training Command

Subj: NAVAL EDUCATION AND TRAINING COMMAND PRIVACY ACT PROGRAM

Ref: (a) 5 U.S.C. §552a
(b) DoD Instruction 5400.11 of 29 January 2019
(c) DoD 5400.11-R, DoD Privacy Program of 14 May 2007
(d) SECNAVINST 5211.5F
(e) SECNAVINST 5239.19A
(f) SECNAVINST 5720.42G
(g) SECNAVINST 5210.8F
(h) Uniform Code of Military Justice
(i) NAVPERS 15560D
(j) OPNAVINST 3500.39D
(k) OPNAVINST F3100.6K
(l) DONCIO memo of 12 Feb 19
(m) Manual of the Judge Advocate General
(n) DONCIO memo of 30 Mar 22
(o) DONCIO memo of 17 Jul 23

Encl: (1) Naval Education and Training Command Headquarters
Privacy Act System of Records
(2) Sample Standard Form 901
(3) Naval Education and Training Command Personally
Identifiable Information Electronic Spillage Report
Process

1. Purpose. To implement references (a) through (o) within the Naval Education and Training Command (NETC) domain; to ensure that all Department of the Navy (DON) military members, civilian employees, contractors, and contractor employees are fully aware of their responsibilities under the provisions of the federal Privacy Act (PA); to balance the government's need to maintain information with the obligation to protect individuals against unwarranted invasion of their privacy stemming from the DON's collection, maintenance, use, and disclosure of personally identifiable information (PII); and to require privacy management practices and procedures be employed to evaluate privacy risks in DON web sites and unclassified non-national

security information systems. Enclosure (1) provides reference for NETC Headquarters (HQ) PA Systems of Records (SOR). Enclosure (2) is a sample of the Controlled Unclassified Information (CUI) Cover Sheet (Standard Form (SF) 901). Enclosure (3) provides guidance on the report process for PII electronic spillage.

2. Cancellation. NETCINST 5211.2D.

3. Background. Reference (a), The PA of 1974, is designed primarily to protect the personal privacy of individuals about whom records are maintained by agencies of the federal government. Reference (b) establishes policy, assigns responsibilities, and prescribes procedures for administering the Department of Defense (DoD) privacy and civil liberties programs. Reference (c) is the regulation for the DoD Privacy Program. The PA is issued within the DON by reference (d). Reference (e) establishes the DON policy on computer incident handling and reporting requirements. The Freedom of Information Act (FOIA), issued by reference (f), is designed to make available to the public information concerning operations, activities, and administration of the DON and other federal agencies without unreasonably invading the privacy rights of any individual. Reference (g) is the policy for the DON Records Management program. Reference (h) is the Uniform Code of Military Justice. Reference (i) is the Naval Military Personnel Manual. Reference (j) establishes policy, guidelines, procedures, and responsibilities to standardize operational risk management (ORM) processes across the Navy. Reference (k) establishes special incident reporting procedures. Reference (l) establishes the DON policy in the event of a known or suspected loss of DON PII. Reference (m) is the Manual of the Judge Advocate General. Reference (n) provides guidance on the forms to utilize if a loss of PII occurs. Reference (o) provides guidance on the mandatory use of the new DoD Wide PII Breach Reporting Tool, Defense Privacy Information Management System (DPIMS).

4. Policy. DON personnel, including contractors and contractor employees, have an affirmative responsibility to protect an individual's privacy when collecting, maintaining, using, or disseminating personal information about an individual.

5. Information. This instruction applies to all NETC employees who use, collect, maintain, or disseminate PII, and also applies to contractors, vendors, or other entities that develop, procure, or use information technology (IT) systems under contract to DON and NETC, to collect, maintain, or disseminate information in identifiable form, or about members of the DON. This instruction governs the collection, safeguarding, maintenance, use, access, amendment, and dissemination of PII by NETC commands and personnel maintained in a DON PA SOR. The provisions of this instruction are punitive in nature and violations may result in disciplinary or administrative action as follows:

a. Military Members. Military members, including reservists on active duty, who violate the provisions of this instruction may be subject to criminal and administrative consequences per the provisions of references (a) and (h). Additionally, military members may be subject to other non-judicial and administrative corrective measures including, but not limited to, processing for administrative separation per the provisions of reference (i).

b. Civilian Employees. Civilian employees are subject to the criminal provisions of reference (a). Additionally, violations of the provisions of reference (a) or this instruction may result in administrative corrective action(s).

c. Contractors

(1) When a Navy or U.S. Government contractor requires the operation of a SOR or a portion of a SOR or requires the performance of any activities associated with maintaining a SOR, including the collection, use, and dissemination of the contents of record systems, the record system or the portion of the record system affected is considered to be maintained by the Navy. The contractor and its employees are considered employees of the Navy for purposes of the criminal provisions of reference (a) during the performance of the contract.

(2) If the contractor must use, have access to, or disseminate PII subject to references (c) and (d) and this instruction in order to perform any part of a contract and the information would have been collected, maintained, used, or

disseminated by the Navy but for the award of the contract, these contractor activities are subject to references (c) and (d) and this instruction.

6. Terms and Definitions. Unless otherwise stated in this instruction, all defined terms listed will have the same meaning as those in references (d) and (l):

a. Breach. A privacy breach is defined as a known or suspected loss of DON PII.

b. Electronic Spillage. An electronic spillage is data placed in an IT system possessing insufficient security controls to protect the data at the required classification. Loss of portable electronic media or the compromise of PII data to unauthorized individuals via e-mail, portable electronic media, shared file services, or other IT is considered an electronic spillage.

c. Lost, Stolen, or Compromised Information. Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personally protected information where persons other than authorized users gain access or potential access to such information for other than authorized purposes, where one or more individuals will or may be adversely affected. Such incidents are also known as breaches or spillages.

d. Maintain. Means to maintain, collect, use, or disseminate.

e. ORM. A decision-making tool to identify, assess, and manage risks.

f. Operation of a SOR. Performance of any of the activities associated with maintaining a SOR, including the collection, use, and dissemination of records.

g. PA Coordinator (PAC). Individual appointed by a command to serve as the principal point of contact (POC) on PA matters.

h. PA Office Administrator. A designated person who has cognizance over any function or program that collects, maintains, or uses PII in a command, department, division, work center, or office.

i. Personal Information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her (e.g., a social security number (SSN); age; military rank; civilian grade; marital status; race; salary; home and office phone numbers; other demographic, biometric, personal, medical, and financial information, etc.). Such information is also known as PII (e.g., information which can be used to distinguish or trace an individual's identity, such as their name, SSN, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual).

j. Portable Electronic Media. Portable electronic media include, but are not limited to, laptops, flash drives, thumb drives, compact discs (CD) and digital video discs (DVD), and cell phones.

k. PA Statement (PAS). Required statement when an individual is requested to furnish personal information for inclusion in a SOR regardless of the medium used to collect the information (paper or electronic forms, personal interviews, telephonic interviews, or other methods). The statement enables the individual to make an informed decision whether to provide the information requested, and should be used whenever personal information is collected. A PAS must include all of the elements found in section C2.1.4.2 of reference (c).

l. Privacy Impact Assessment (PIA). An ongoing assessment to evaluate adequate practices in balancing privacy concerns with the security needs of an organization. The process is designed to guide owners and developers of information systems in assessing privacy through the early stages of development. The process consists of privacy training, gathering data from a project on privacy issues, identifying and resolving the privacy risks, and approval by the information systems security manager (ISSM).

m. Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc.), about an individual that is maintained by a DON activity including, but not limited to: the individual's education, financial transactions, medical, criminal, or

employment history, and that contains the individual's name or other identifying particulars assigned to the individual, such as a finger, voice print, or a photograph.

n. Spillage. The Navy defines spillage as placing classified data on a lower-order classified computer. PII data placed on improperly classified and protected IT systems data storage media constitutes an electronic spillage of PII.

o. SOR Manager. An official who has overall responsibility for a SOR. They may serve at any level in DON. SOR managers are indicated in the published record systems notices. If more than one official is indicated as a SOR manager, initial responsibility resides with the manager at the appropriate level (e.g., for local records, at the local activity).

p. SOR Notice (SORN). A group of records under the control of a DON activity from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all PA SORs must be published in the Federal Register and are also available for viewing or downloading from the Navy's PA online web site at <https://www.doncio.navy.mil> (select "Privacy" link).

7. PA. Any misuse or unauthorized use of PII may result in both civil and criminal penalties. All collection, use, maintenance, or dissemination of PII will be in accordance with reference (a), as amended.

8. Responsibilities

a. NETC Force Judge Advocate (FJA) (N00J)

(1) Designated as the NETC PAC to perform the duties in paragraph 7h of reference (d) for all NETC commands and activities.

(2) The principal POC for all PA matters for the NETC domain including, but not limited to, reporting PII breaches and acting as the POC for all follow-up actions and individual notifications regarding any breach. Commands and activities subordinate to NETC (excluding Navy Recruiting Command and Naval

Service Training Command) must contact the NETC PAC in the event of any actual or suspected breach and shall act only through the PAC.

(3) Provide assistance when notified by a command, activity, department, or PA system administrator of the need to establish a new Navy PA SOR, amend or alter an existing Navy SOR, or delete a Navy SOR that is no longer needed.

(4) Semi-annually, in April and October, conduct a command-wide review of NETC PA practices to determine compliance with all requirements and to ensure that basic PII safeguards are in place. This review will be conducted utilizing the PII Spot Check form approved and provided by the PAC. The review must include, but not be limited to:

(a) Compliance with all PA training requirements.

(b) Identification in writing of all PA administrators (previously identified as PA POCs) and SOR administrators.

(5) Process PA complaints.

(6) Publish and maintain NETC HQ PA SORs (enclosure (1)).

b. Commands

(1) Review annually, or more frequently, internal directives, forms, practices, and procedures, including those having PA implications and where PAS are required for solicited PII. Special attention is directed to command and classroom indoctrination process personal information requests (e.g., name, address, home phone number, cell phone number, spouse and children names and contact info) and command or staff duty binder recall rosters (e.g., name, address, home phone number, and cell phone number) as well as any internal or local programs that screen candidates or otherwise collect information.

(a) Review annually, or more frequently, the necessity of the use of laptops and portable electronic media (e.g., external drives, CDs and DVDs, diskettes, and phones and personal digital assistants) and establish practices and

procedures, including written authorization, for the use of laptops, portable electronic media or other portable electronic devices, which may contain PII, outside DoD assigned, authorized, or furnished work spaces.

(b) Incorporate ORM (reference (j)) as an integral part of the decision process to identify, assess, and manage risks associated with the collection, storage, maintenance, and use of PII.

(2) Appoint a command PAC in writing.

(3) Appoint PA office administrators in writing.

(4) Ensure no official files are maintained that are retrieved by an individual's name or other personal identifier without first ensuring that a SORN exists that permits such collection.

(5) Ensure PA system administrators are properly trained on their responsibilities for protecting PII being collected, maintained, and disseminated under the DON PA program.

(6) Consistent with the Federal Acquisition Regulations (FAR), ensure contracts for the operation of a SOR identify specifically the record system and the work to be performed, and include in the solicitation and resulting contract the terms as prescribed by the FAR, including how PII data is to be disposed of at the end of the contract. Inform contractors of their responsibilities regarding the DON PA program and ensure they understand PII and comply with all protocols for handling PII.

(7) Work closely with the public affairs officer (PAO) and web master to ensure that PII is not placed on public web sites or in public folders.

(8) Annually conduct reviews of PA SORs to ensure that they are necessary, accurate, and complete.

(9) Review and validate PIAs for information systems for submission to Chief of Naval Operations (CNO) (DNS-36).

(10) Maintain liaison with records management officials (e.g., maintenance and disposal procedures and standards, forms, and reports), as appropriate.

(11) Ensure assigned personnel (military, civilian members and contractors) receive mandatory Navy Privacy training within 30 days of reporting for military duty or employment by the command. Civilians and contractors are required to complete the Navy Privacy Training annually. (Contractor employees should refer to their DON contract for their specific requirements). Military personnel will follow guidance placed in annual NAVADMIN releases on general military training requirements.

(12) Ensure that DON Chief Information Officer (DON CIO) required bi-annual PII spot checks are completed, usually in April and October, reviewed by the commanding officer or officer in charge in a timely manner, and kept on file at the command as an auditable record for 3 years. Do not wait for NETC direction to complete the spot checks; initiate them at the appropriate place and time to accurately check command compliance. Report completion of spot checks to NETC FJA.

(13) Breach reporting is a required action when there is a known or suspected loss of DoD PII per reference (o). The DoD has modernized PII breach reporting by moving to a new, automated DoD wide PII breach reporting tool called DPIMS. This new tool is now a digital and fillable version of the current DoD PII Breach Reporting Form, DD 2959. DPIMS will allow anyone with a DoD common access card (CAC) to submit a PII breach report for more timely reporting and allow the submitter to receive breach notifications of actions taking place from initial reporting to closure of the report. Effective 17 July 2023, DON organizations and personnel will use the new DPIMS for submitting a PII breach. First time users with DoD CACs will need to register first before using the portal. Register using the Defense Information Systems Agency Services Portal at <https://services.disa.mil>, or by contacting 1-844-347-2457, option 1. Users will receive an e-mail notice upon approval. Upon successful login during the initial report, users from both Navy and Marine Corps will use the pull down menu to select the component (U.S. Navy). For sub-component Navy personnel will

select the appropriate echelon 2 command, for Marine Corps submissions under sub-component select United States Marine Corps.

(14) Expeditiously report all actual or potential lost, stolen, or compromised PII, including breaches and spillages, following the steps in enclosure (3), as follows:

(a) Affected command will report breaches and spillages electronically using DPIMS for initial and supplemental reporting. Once a breach report has been submitted, the echelon 2 command PAC will receive and send notification via DPIMS and prepare an echelon 2 risk assessment via DPIMS prior to final submission to DON CIO. DON CIO will review the report either direct further action or close out the report as complete. If commission of a crime is suspected, notify the local Naval Criminal Investigative Service office or Marine Corps Criminal Investigative Investigation Division to conduct an investigation.

(b) If the breach involved the loss or suspected loss of a government authorized credit card or associated financial data associated with a card, immediately notify the issuing bank, and the command's government credit card manager.

(c) Within 24 hours after receipt, the DON CIO privacy office will review the initial breach report and determine the potential risk of harm to impacted personnel. Based on the review, the DON CIO privacy office will notify the organization's designated official of the required notification, if any.

(d) OPREP-3: Issue, if appropriate, per reference (k).

(e) Notifications, if required, are to be made within 10 days of the discovery of loss or suspected loss of PII. The designated official must, by written letter or digitally signed e-mail, notify all impacted individuals. A sample notification letter is available at <http://doncio.navy.mil> ("Privacy" link). If the 10 day requirement is not met, the designated official must notify the DON CIO privacy office, provide the reason why notification was not made, and what actions are being taken to complete the notification process.

For all incidents that require notification, the command or activity is directed to investigate whether DON policy was followed. In cases where policy was not followed, appropriate disciplinary action should be taken, weighing mitigating circumstances, severity of the PII loss or compromise, and other extenuating factors.

(15) Investigate all actual or potential instances of lost, stolen, or compromised PII per chapter 2 of reference (m). Investigations will identify the root cause, assess responsibility and accountability, and recommend measures and actions to prevent recurrence.

(16) Ensure disposal of records from SORs to prevent inadvertent disclosure. Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (e.g., tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation). Magnetic media may be cleared by completely erasing, overwriting, or degaussing the tape. Although PA data may be recycled, it must be shredded prior to being sent for recycling.

(17) Echelon 2 and 3 commands will issue a PA implementing instruction. All other commands will publish command guidance. Instructions or guidance will:

- (a) Identify the command PAC.
- (b) Address PA records disposition.
- (c) Address PA processing procedures.
- (d) Identify those SORs being used by the activity.
- (e) Provide training and guidance to those personnel involved with collecting, maintaining, using, or disseminating information from a PA SOR.
- (f) Provide guidance and notification procedures if there is an actual, potential, or suspected loss, theft, or compromise of PII.

c. Command PAC

(1) Serve as principal POC on PA matters.

(2) Provide initial overview and annual training to staff personnel on the provisions of references (a) through (g).

(3) Provide assistance when notified of the need to establish a new Navy PA SOR, amend or alter an existing Navy SOR, or delete a Navy SOR that is no longer needed. Notify and coordinate with immediate superior in command PAC(s) and CNO (DNS-36).

(4) Process all PA requests. Provide guidance to command personnel on handling PA requests, scope of PA exemptions, and the fees, if any, that may be collected.

(5) Process PA complaints.

(6) Complete and maintain a disclosure accounting form for all disclosures made.

d. CIO, N6, and ISSM

(1) Provide guidance for effective assessment and utilization of privacy-related technologies.

(2) Provide guidance to properly protect PII on portable storage devices and ensure portable storage devices do not contain any PII unless properly protected pursuant to that guidance.

(3) Provide guidance on the conduct of PIAs and oversee command PIA policy and procedures to ensure PIAs are conducted commensurate with the information system being assessed, the sensitivity of PII in that system, and the risk of harm for unauthorized release of that information. DON CIO reserves the right to request that a PIA be completed on any system that may have privacy risks.

(4) Review all command PIAs prior to approval by the DON CIO.

(5) Develop and coordinate privacy policy, procedures, education, training, and awareness practices regarding NETC information systems.

(6) Ensure NETC compliance with DON web and information systems privacy requirements, including use of encryption software and implementation of prescribed privacy-related technologies.

(7) Provide input as required for inclusion in the Federal Information Systems Management Act Report.

e. NETC PAO. The NETC PAO shall ensure NETC compliance with DON world wide web privacy requirements.

f. Department PACs and Administrators. Department PACs will be designated by their department. Departments with offices located outside the Pensacola area will designate a PA assistant who will liaise with the department PAC. Department PACs will:

(1) Establish appropriate administrative, technical, and physical safeguards to ensure the records in SORs that are maintained or used are protected from unauthorized alteration, destruction, or disclosure. Protect the records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. Ensure safeguards are in place to protect the privacy of individuals and confidentiality of PII contained in a SOR. Use the ORM process (reference (j)) to identify, assess, and manage risks to PII.

(2) Require use of a SF 901 on all documents and files containing PII.

(3) Double wrap mail containing PII. Address internal wrapper for intended recipient and mark "CONTROLLED UNCLASSIFIED INFORMATION."

(4) Ensure addition of "CUI" at the top and bottom of each page of a document containing PII. Additionally, apply a CUI information block on the bottom right area of the first page of each document that contains CUI.

(5) Work with IT personnel to identify any new information systems being developed that contain PII. If a PA SORN does not exist to allow for the collection, notify the system administrator who will assist in creating a new SORN that permits collection. The program manager will ensure that each newly proposed PA SORN is evaluated for need and relevancy and confirm that no existing PA SORN covers the proposed collection. Ensure that no illegal files are maintained.

(6) Ensure records are kept per retention and disposal requirements set forth in reference (g) and are maintained per the identified PA SORN.

(7) Work closely with the PAC to ensure that all personnel who have access to a PA SOR are properly trained on their responsibilities under the PA. Ensure that only those DoD and DON officials with an "official need to know" in the performance of their duties have access to information contained in a SOR.

(8) Identify all SORs that are maintained, in whole or in part, by contractor personnel, and ensuring that they are properly trained.

(9) Take reasonable steps to ensure the accuracy, relevancy, timeliness, and completeness of records that may be disclosed to anyone outside the federal government. Stop collecting any category or item of information about individuals that is no longer justified and, when feasible, remove the information from existing records.

(10) Routinely inspect, not less than quarterly, all SORs within the PA office administrator's area of responsibility, including records maintained wholly or in part by contractor personnel, for PA compliance.

(11) Review annually each PA SORN used to determine if they are current and are used in matching programs and are in compliance with the Office of Management and Budget guidelines. If changes are required, coordinate with the PAC. Changes to SORNs not under the cognizance of NETC should be reported to the appropriate system manager.

(12) With the assistance of the ISSM, complete and maintain a PIA for those systems that collect, maintain, or disseminate PII according to DoD and DON guidance.

(13) Immediately notify the PAC when there is a request for PA information.

(14) Immediately notify the PAC and command when there is an actual, potential, or suspected loss, theft, or compromise of PII.

g. NETC Inspector General (IG) (N00G)

(1) During assistance visits, reviews, or inspections within NETC HQ staff and lower echelon commands, test compliance with PA guidelines. Recommend, when necessary, remedies to correct noted internal control weaknesses.

(2) When performing the above, evaluate the effectiveness of staff and command protocols for preventing instances of loss, theft, or compromise of PII. Test the procedures used to take immediate action should a loss occur. Determine the effectiveness of command protocols for rapidly reporting a possible loss, theft, or compromise and informing affected individuals how to ensure their identity has not been compromised.

(3) During inspections of lower echelon commands, evaluate managerial efforts to protect PA data embedded in command processes. Determine the level of compliance with the DON Managers' Internal Control Program (MICP). Ensure MICP documentation shows the steps employed to protect processes from potential internal control breakdowns in safeguarding PA data.

h. NETC Personnel (including contractors)

(1) Ensure that PII which is accessed or used to conduct official business is protected so the security and confidentiality of the information is preserved. Use ORM process to identify, assess, and manage risks to PII accessed or used.

(2) Do not disclose any information contained in a SOR by any means of communication to any person or agency, except as authorized by references (a) through (g) or the specific PA SORN.

(3) Do not request or collect any PII except as authorized by a specific PA SORN. Prior to collecting PII from an individual, a PAS shall be provided to the individual.

(4) Do not maintain unpublished official files that would fall under the provisions of reference (a).

(5) Safeguard the privacy of individuals and confidentiality of PII contained in SORs.

(6) Transmittal and emailing PII. In those instances where transmittal of PII is necessary, the originator must take every step to properly mark the correspondence so that the receiver of the information is apprised of the need to properly protect the information.

(a) Require the use of SF 901, see enclosure (2) for sample, on hard copy documents or files containing PII.

(b) Emailing of PII must be digitally signed and encrypted using current approved certificates. Ensure the subject line opens with, "CUI:"

(7) Do not maintain PII or privacy sensitive information in unrestricted public folders.

(8) Do not maintain or store PII on portable electronic media (e.g., laptops, flash drives, thumb drives, CD and DVD, diskettes, iPhones, or other portable electronic devices) unless:

(a) All files, documents, and products containing PII on laptops and portable electronic media are encrypted using current approved encryption methods; or

(b) The laptop and portable electronic media contains records on 25 individuals or less; and

(c) The command has provided written authorization to utilize the laptop and portable electronic media containing PII outside DoD assigned, authorized, or furnished work spaces. Use the ORM process (reference (j)) to identify, assess, and manage risks to PII possessed or used outside the normally assigned, authorized, or furnished government work space.

(d) Portable electronic media must be protected at all times. Individuals using or traveling with laptops and portable electronic media will maintain positive control of the laptop and media at all times. Laptops and portable electronic media will not be placed in checked luggage or left in unoccupied vehicles at any time. When utilizing government, commercial, or private lodging, laptops and portable electronic media will be secured inside a locked room and, if available, stored in a locked container.

(e) Do not maintain, store, or process PII on personal or non-government owned and provided and authorized computers (including hotel, internet café, library or other non-government computers), network systems, portable electronic media (e.g., laptops, flash drives, thumb drives, CD and DVD, diskettes, iPhones), or other portable electronic devices.

(9) Immediately report any actual, suspected, or potential loss, theft, compromise, breach, or spillage of PII to the PA office administrator, command PAC, and command.

(10) Report any unauthorized disclosure of PII from a SOR to the command and command PAC.

(11) Report the maintenance of any unauthorized SORs to the PAC.

(12) Dispose of records from SORs to prevent inadvertent disclosure. Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (e.g., tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or reconstruction). Magnetic media may be cleared by completely erasing, overwriting, or degaussing the tape. Although PA data may be recycled, it must be shredded prior to being sent for recycling.

9. Processing PA Requests. Records protected by the PA must be released only to those with a need to know. All requests for a release of records to anyone outside DoD must be referred to the PAC for a release determination. Frequently, the requested records will contain information partially unsuited for release because it pertains to a third party, or falls under another recognized exception to reference (a). Therefore, under no circumstances will any records be released to anyone outside of DoD prior to such a determination.

10. PA Team. A NETC HQ PA team chaired by NETC (N00J), consisting of representatives from NETC HQ (N00J, N00G, N00D, N6, and N04), and others assigned will meet at least quarterly, or on a less frequent basis, if determined appropriate by N00J, to identify and prevent inadvertent releases of unauthorized disclosures of PII and to establish best business practices.

11. Web sites. All personnel (including contractors) are required to be familiar with references (a) through (g) and are encouraged to routinely visit the DON PA, FOIA, and CIO web sites to learn of the most current news, developments, and guidance.

12. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the DON Assistant for Administration, Directives and Records Management Division portal page at <https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx>.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager.

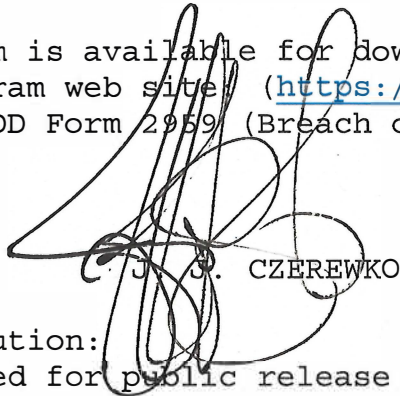
13. Review and Effective Date. Per OPNAVINST 5215.17A, NETC will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, DoD, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 (Review of Instruction). This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued

by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

14. Forms

a. The following form is available for download from U.S. General Services Administration web site: (<https://www.gsa.gov/reference/forms/>): SF 901 (CUI Cover Sheet)

b. The following form is available for download from the DoD Forms Management Program web site (<https://www.esd.whs.mil/Directives/forms/>): DD Form 2959 (Breach of PII)



C. J. CZEREWKO

Releasability and distribution:
This instruction is cleared for public release and is available electronically on the NETC public web site (www.netc.navy.mil) or by e-mail at netc-directives@us.navy.mil

NAVAL EDUCATION AND TRAINING COMMAND HEADQUARTERS PRIVACY ACT
SYSTEMS OF RECORDS

SORN Uniform Resource Locator: <https://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/NavyUSMC-Article-List/>

N01301-2	On-Line Distribution Information System
NM01500-10; DoD-0005	Navy Training Management and Planning System; Defense Training Records
NM01650-1	DON Military Awards System
NM05000-1	General Correspondence Files
NM05000-2	Program Management and Locator System
N05041-1	Naval IG Investigative Records
NM05100-5	Enterprise Safety Applications Management System
NM05211-1; DoD-0008	PA Request/Amendment Files and Tracking System
N05350-1	Navy Drug and Alcohol Program System
N05354-1	Military Equal Opportunity Network
NM05512-1	Vehicle Parking Permit and License Control System
N05520-5	Personnel Security Program Management Records System
NM05720-1; DoD-0008	FOIA Request/Appeal Files and Tracking System
N05800-1	Legal Office Litigation/Correspondence File
N05810-2 DoD-0006	Military Justice Correspondence and Information File
N05813-6	Summary and Non-BCD Special Courts-Martial Records of Trial
N05819-4	Complaints of Wrong Under Article 138 or Article 1150
N05830-1	JAG Corps Manual Investigative Records
N05891-1	JAG Litigation Case File
N06110-1	Physical Readiness Information Management System
NM07421-1	Time and Attendance Feeder Records
NM12610-1	Hours of Duty Records
NM12711-1	Labor Management Relations Records System
EEOC/GOVT-1	Equal Employment Opportunity in the Federal Government Complaint and Appeal Records
GSA/GOVT-4	Contracted Travel Services Program
MSPB/GOVT-1	Appeals and Case Records
OGE/GOVT-1	Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records

NETCINST 5211.2E
17 Oct 2024

OGE/GOVT-2	Executive Branch Confidential Financial Disclosure Reports
OPM/GOVT-1	General Personnel Records
OPM-GOVT-2	Employee Performance File System Records
OPM/GOVT-3	Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers
OPM/GOVT-5	Recruiting, Examining, and Placement Records
OPM/GOVT-7	Applicant Race, Sex, National Origin, and Disability Status Records
NM01500-2	DON Education and Training Records
A0351 DAPE	Army Training Requirements and Resources System
DMDC-01	Defense Manpower Data Center Data Base
DSCA 06	Defense Security Assistance Management System
N01080-1	Enlisted Master File Automated Systems
NM11101-1	Family and Unaccompanied Housing Program
N07220-1	Navy Standard Integrated Personnel System
M01754-6	Exceptional Family Member Program Records
N01080-2	Officer Master File Automated Systems
N01080-3	Reserve Command Management Information
M01040-3	Marine Corps Manpower Management Information System Records
79 FR 8489	Department of Labor Registered Apprenticeship Partners Information Database System (interface partner)
A0600-8-104AHRC	Army Personnel System
N01131-1	Officer Selection and Appointment System
N01306-1	Career Management System - Interactive Detailing
N01133-1	NAME/LEAD Processing System
N01133-2	Recruiting Enlisted Selection System
N01533-2	Navy Junior Reserve Officer Training Corps Payment Reimbursement System

SAMPLE STANDARD FORM 901

CUI

ATTENTION

Use this space to indicate categories, limited dissemination controls,
special instructions, points of contact, etc., if needed.

Controlled by:
Controlled by:
CUI Category:
Distribution/Dissemination Control:
POC:

ATTENTION

All individuals handling this information are required to protect
it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must
be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of Controlled Unclassified Information shall be
allowed as necessary and permissible to any individual(s), organization(s), or
grouping(s) of users, provided such access or dissemination is consistent with or in
furtherance of a Lawful Government Purpose and in a manner consistent with
applicable law, regulations, and Government-wide policies.

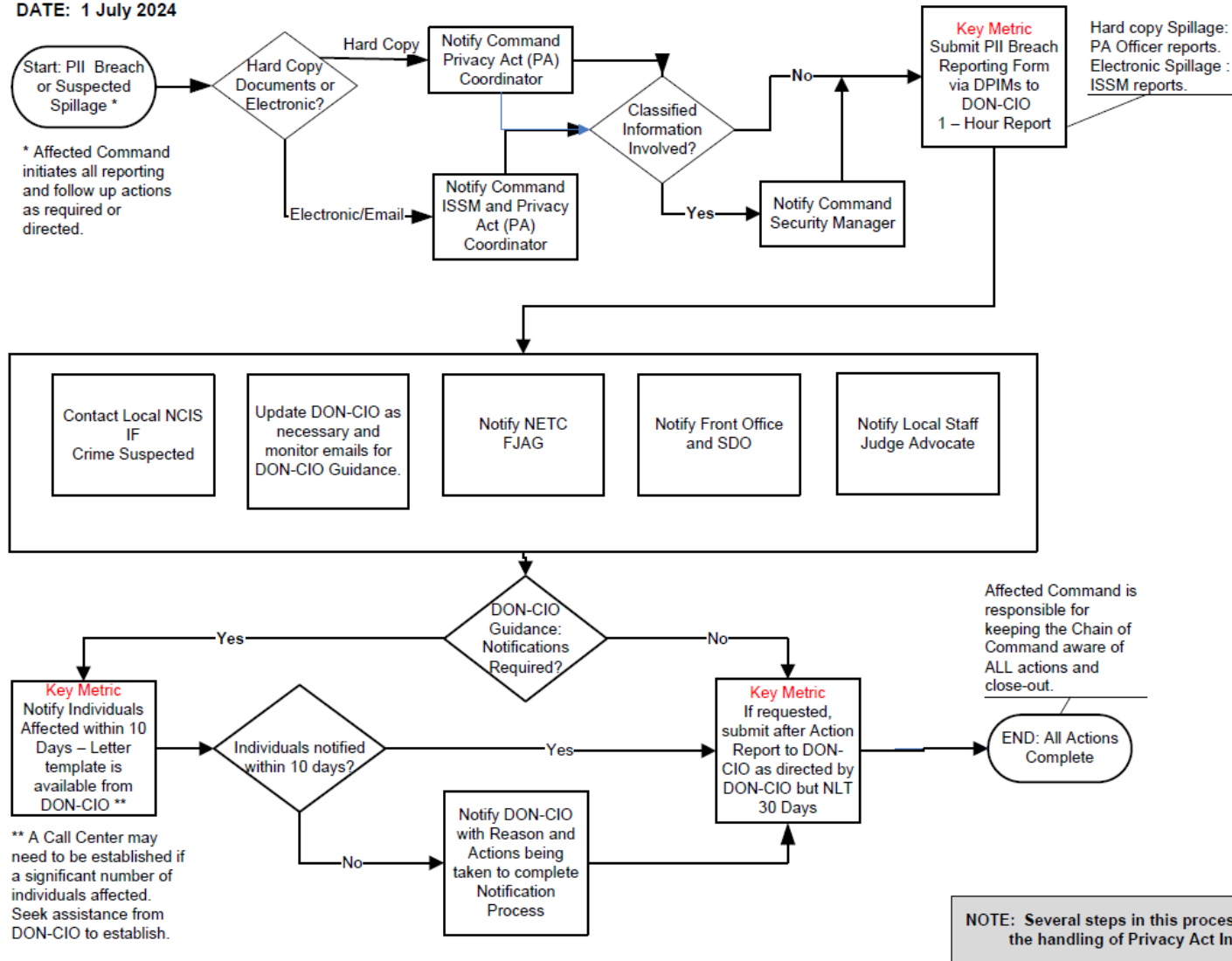
Standard Form 901 (11-10)
Prescribed by GSA/ISOO | 32 CFR 2002

CUI

(Unclassified - For illustration purposes only.)

NAVAL EDUCATION AND TRAINING COMMAND PERSONALLY IDENTIFIABLE INFORMATION ELECTRONIC
SPILLAGE REPORT PROCESS

Purpose: Process by which Loss of Personally Identifiable Information is reported Per DON-CIO 291652Z Feb 2008
Process Owner: Naval Education and Training Command, N00JC,
COM: (850) 452-4847
DATE: 1 July 2024



Reviewed: 1 July 24