DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

ISES-SEC-PV-054

ISES-RMZ (25-1aaaaa1)

20 November 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Privacy Impact Assessment Guidance

1. References. See enclosure 1.

2. Purpose. This memorandum establishes the guidelines for Privacy Impact Assessments (PIAs).

3. Background.

a. For the purposes of this policy, Information Technology (IT) is defined as Army-owned IT and Army controlled IT. Army IT includes Information Systems (IS), Platform Information Technology (PIT), IT products and services (see enclosure 2 for definitions).

b. Privacy Impact Assessment (PIA) (DD Form 2930) is part of the process that helps organizations identify and manage the privacy risks associated with IT and electronic collections. The PIA will serve as a conclusive determination of whether PII is collected by the IT in order to ensure compliance with applicable privacy requirements.

c. The E-Government Act of 2002, requires federal agencies to evaluate IT and electronic collections that collect personally identifiable information (PII) and determine whether the privacy of that PII is adequately protected.

d. A PIA is an analysis of how PII is collected, used, shared, and maintained. This helps ensure that individuals are informed about the data gathered on them, any effects IS may have on personal privacy are effectively managed, and only the necessary amount of personal information required for program administration is collected.

4. Policy.

a. PIA Requirements:

(1) IT and electronic collections that collect PII are accounted for and authorized to collect PII.

(2) IT and electronic collections are required to go through the appropriate governance process and receive approval by the appropriate System Mission Area.

(3) Networks, Data Centers, Platform Information Technology (PIT), weapons systems, and Industrial control systems do not require the completion of a PIA. Authorizing Officials

and System Owners are encouraged to use the PIA to document privacy implementation considerations.

(4) National Security Systems (NSS) do not require the completion of a PIA. For NSS that process PII, Authorizing Officials and System Owners are encouraged to use the PIA to document privacy implementation considerations.

(5) Review and update PIAs every 3 years or when there is a significant system change or a change or shift in privacy or security posture, for IT and electronic collections regardless of form or format.

b. No Collect PIAs

(1) IT and electronic collections that do not collect PII still require a PIA.

(2) The purpose of this PIA is to validate and document that the IT and electronic collections does not collect PII and to ensure that the system's record-keeping processes are accountable, and the retention periods for these records are properly documented.

5. Submit all PIAs, with the exception of those described in paragraph 4a(3)–(4), to usarmy.belvoir.hqda-cio.mbx.armd-apclb-pia-sorn-ssnj@army.mil. PIAs will be reviewed for records management, information collection, and privacy implications. All PIAs, with the exception of those described in paragraph 4a(3)–(4), are approved by the Army CIO.

6. Review. The Army Records Management Directorate (ARMD) will review this memorandum annually for potential changes to policy.

7. Points of contact:

a. CIO Policy Inbox: usarmy.pentagon.hqda-cio.mbx.policy-inbox@army.mil.

b. ARMD: Ms. Joyce Luton, ARMD Director at phone (703) 473-0613 and email joyce.luton2.civ@army.mil.

GARCIGA.LEONEL.T.1186170411
Digitally signed by GARCIGA.LEONEL.T.1186170411
Date: 2024.11.20 16:33:38 -05'00'

Encls

LEONEL T. GARCIGA
Chief Information Officer

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
(CONT)

DISTRIBUTION: (CONT)
- U.S. Army Futures Command
- U.S. Army Pacific
- U.S. Army Europe and Africa
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Army Cyber Command
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Human Resources Command
- U.S. Army Corrections Command
- U.S. Army Recruiting Command

Superintendent, U.S. Military Academy
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency
Executive Director, Military Postal Service Agency
Director, U.S. Army Criminal Investigation Division
Director, Civilian Protection Center of Excellence
Director, U.S. Army Joint Counter-Small Unmanned Aircraft Systems Office
Superintendent, Arlington National Cemetery
Director, U.S. Army Acquisition Support Center

CF:
Principal Cyber Advisor
Director of Enterprise Management
Director, Office of Analytics Integration
Commander, Eighth Army

REFERENCES

a. OMB M-03-22 (OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002). Available at: https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf

b. DoDI 5400.16 (DoD Privacy Impact Assessment (PIA) Guidance). Available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/540016p.pdf?ver=2019-08-12-133733-200

c. AR 25-1 (Army Information Technology). Available at: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN37510-AR_25-1-001-WEB-3.pdf

d. Pam 25-1-1 (Army Information Technology Implementation Instructions). Available at: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36806-PAM_25-1-1-001-WEB-3.pdf

e. NIST SP 800-82r3 (Guide to Operational Technology (OT) Security). Available at: https://csrc.nist.gov/pubs/sp/800/82/r3/final

DEFINITIONS

Army Controlled: Used only for Army purposes, dedicated to Army processing, and effectively under Army configuration control. Source: DoDI 8500.01

Industrial Control Systems: General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations that are often found in the industrial sectors and critical infrastructures, such as programmable logic controllers (PLC). An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). Source: NIST Special Publication 800-82r3 (Guide to Operational Technology (OT) Security)

Information Technology: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used directly or is used by a contractor under a contract with the executive agency, which 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" also includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a federal contractor incidental to a federal contract. [Reference 40 USC Subtitle III (Clinger-Cohen Act of 1996)]. Source: AR 25-1 (Army Information Technology)

IT product: Individual IT hardware or software items. Products can be commercial, or government provided and include, but are not limited to, operating systems, office productivity software, firewalls, and routers. Source: DoDI 8500.01

IT Service: A capability provided to one or more DoD entities by an internal or external provider based on the use of information technology and that supports a DoD mission or business process. An IT Service consists of a combination of people, processes, and technology. Source: DoDI 8500.01

National Security System: As defined in the Clinger-Cohen Act, an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management. (Source: OMB M-03-22)

Operational Technology: A broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical

environment monitoring systems, and physical environment measurement systems. Source: NIST Special Publication 800-82r3 (Guide to Operational Technology (OT) Security)

Personally Identifiable Information: 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. (Source OMB Circular No A-130)

Platform Information Technology: Refers to computer resources, both hardware and software, which are physically a part of, dedicated to, or essential in real time to the mission performance of special-purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility-distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration. Source: AR 25-1 (Army Information Technology)

System Mission Area: A defined area of responsibility whose functions and processes contribute to accomplishment of the mission. Those mission areas are: The Warfighting Mission Area (WMA), Business Mission Area, (BMA), Defense Intelligence Mission Area (DIMA), and Enterprise Information Environment Mission Area (EIEMA). (DoDD 8115.01)