Information Technology (IT) System Personally Identifiable Information Processing and Transparency (PT) Standard

January 31, 2022

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2022.02.01 16:07:10 -05'00'

Steven Hernandez
Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Date	Summary of Changes
1.0	1/18/2022	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with the EO.

Table of Contents

1 INTRODUCTION

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing regulation Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as baseline information system controls.

This governance document establishes Department information technology (IT) system personally identifiable information processing and transparency controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders, Emergency Orders, Binding Operational Directives, and Department Administrative Communications System (ACS) directives and policies. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these personally identifiable information processing and transparency control standards.

2 STANDARDS

The Department standards for IT system personally identifiable information processing and transparency controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS 199 categorization level (e.g., Low (L), Moderate (M) and High (H)) is assigned to each requirement. This designator indicates a requirement applies to information systems

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

categorized at that FIPS 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS 199 impact-level or privacy baseline. In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA).

This standard directly supports the Department's integration of the NIST Cyber Security Framework (CSF) in focusing on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to Appendix A for a summary of controls by baseline and corresponding NIST CSF categories and subcategories.

2.1 PT-1 Policy and Procedures (P)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in OCIO: 3-112/ACSD-OCIO-004, *Cybersecurity Policy* a Department-level personally identifiable information processing and transparency policy (e.g., this document) that:

(a) addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

(c) authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as OCIO: 3-112/ACSD-OCIO-004, Cybersecurity Policy.

The Department CISO in conjunction with the Department Senior Agency Official for Privacy (SAOP) is designated to manage the development, documentation, and dissemination of the Department-level personally identifiable information processing and transparency policy.

This policy shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

The Department-level personally identifiable information processing and transparency standard operating procedures shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

2.2 PT-2 Authority to Process Personally Identifiable Information (P)

a. Determine and document the authority as defined in the Privacy Impact Assessment (PIA) that permits the processing as defined in the PIA of personally identifiable information (PII); and

b. Restrict the processing as defined in the PIA of PII to only that which is authorized.

2.3 PT-3 Personally Identifiable Information Processing Purposes (P)

a. Identify and document the purposes as defined in the PIA for processing PII;

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the processing of data as defined in the PIA of PII to only that which is compatible with the identified purpose(s); and

d. Monitor changes in processing PII and implement mechanisms as defined in the PIA to ensure that any changes are made in accordance with existing ED privacy policies.

2.4 PT-4 Consent (P)

Implement mechanisms as defined in the PIA for individuals to consent to the processing of their PII prior to its collection that facilitate individuals' informed decision-making.

2.5 PT-5 Privacy Notice (P)

Provide notice to individuals about the processing of PII that:

a. Is available to individuals upon first interacting with an organization, and subsequently at when changes to the processing of PII requires notification;

b. Is clear and easy-to-understand, expressing information about PII processing in plain language;

c. Identifies the authority that authorizes the processing of PII;

d. Identifies the purposes for which PII is to be processed; and

e. Includes other information as stated in the PIA.

2.5.1 PT-5(2) Privacy Notice | Privacy Act Statements (P)

Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

2.6 PT-6 System of Records Notice (P)

For systems that process information that will be maintained in a Privacy Act system of records:

a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;

b. Publish system of records notices in the Federal Register; and

c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

2.6.1 PT-6(1) System of Records Notice | Routine Uses (P)

Review all routine uses published in the system of records notice biennially to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.

2.6.2 PT-6(2) System of Records Notice | Exemption Rules (P)

Review all Privacy Act exemptions claimed for the system of records at biennially to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.

2.7 PT-7 Specific Categories of Personally Identifiable Information (P)

Apply any processing conditions as defined in the PIA for specific categories of personally identifiable information.

2.7.1 PT-7(1) Specific Categories of Personally Identifiable Information | Social Security Numbers (P)

When a system processes Social Security numbers:

a. Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;

b. Do not deny any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his or her Social Security number; and

c. Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

2.7.2 PT-7(1) Specific Categories of Personally Identifiable Information | First Amendment Information (P)

Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

2.8 PT-8 Computer Matching Requirements (P)

When a system or organization processes information for the purpose of conducting a matching program:

a. Obtain approval from the Data Integrity Board to conduct the matching program;

b. Develop and enter into a computer matching agreement;

c. Publish a matching notice in the Federal Register;

d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and

e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

4 ACRONYMS

ACS	Administrative Communication System
AO	Authorizing Official
ATO	Authorization to Operate
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
DHS	Department of Homeland Security
ED	Department of Education
EO	Executive Order
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
IAS	Information Assurance Services
ISO	Information System Owner
ISSO	Information Systems Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PO	Principal Office
RAF	Risk Acceptance Form
SAOP	Senior Agency Official for Privacy

5 APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below. NIST SP 800-53 controls that are not applicable to any control baseline are shaded in gray.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
PT-1	Policy and Procedures	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CM.PO-P, GV.PO-P, GV.MT-P	ID.IM-P5, CT.PO-P1, CT.PO-P3, CM.PO-P1, CM.PO-P2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6
PT-2	Authority to Process Personally Identifiable Information	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1
PT-2(1)	Authority to Process Personally Identifiable Information | Data Tagging		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1
PT-2(2)	Authority to Process Personally Identifiable Information | Automation		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1
PT-3	Personally Identifiable Information Processing Purposes	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1
PT-3(1)	Personally Identifiable Information Processing Purposes | Data Tagging		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1
PT-3(2)	Personally Identifiable Information Processing Purposes | Automation		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1
PT-4	Consent	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CT.PO-P, CM.AW-P	CT.PO-P1, CT.PO-P3, CM.AW-P8
PT-4(1)	Consent | Tailored Consent		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CT.PO-P, CM.AW-P	CT.PO-P1, CT.PO-P3, CM.AW-P8
PT-4(2)	Consent | Just-in-time Consent		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CT.PO-P, CM.AW-P	CT.PO-P1, CT.PO-P3, CM.AW-P8

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
PT-4(3)	Consent | Revocation		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CT.PO-P, CM.AW-P	CT.PO-P1, CT.PO-P3, CM.AW-P8
PT-5	Privacy Notice	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CM.PO-P, CM.AW-P	CM.PO-P1, CM.AW-P1, CM.AW-P3
PT-5(1)	Privacy Notice | Just-in-time Notice		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CM.PO-P, CM.AW-P	CM.PO-P1, CM.AW-P1, CM.AW-P3
PT-5(2)	Privacy Notice | Privacy Act Statements	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CM.PO-P, CM.AW-P	CM.PO-P1, CM.AW-P1, CM.AW-P3
PT-6	System of Records Notice	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CM.PO-P	CM.PO-P1
PT-6(1)	System of Records Notice | Routine Uses	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CM.PO-P	CM.PO-P1
PT-6(2)	System of Records Notice | Exemption Rules	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CM.PO-P	CM.PO-P1
PT-7	Specific Categories of Personally Identifiable Information	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, ID.RA-P	ID.IM-P6, ID.RA-P1
PT-7(1)	Specific Categories of Personally Identifiable Information | Social Security Numbers	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, ID.RA-P	ID.IM-P6, ID.RA-P1
PT-7(2)	Specific Categories of Personally Identifiable Information | First Amendment Information	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, ID.RA-P	ID.IM-P6, ID.RA-P1
PT-8	Computer Matching Requirements	x	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines		