Personally Identifiable Information (PII)

Developed By **Karen Baez**

Copyright CyberAdeptness LLC

OBJECTIVE

The objective of this presentation is to:

1) Understand the Federal Requirements associated with handling PII Data, whether it is held by Government Agency's and/or 3rd Party Service Providers doing business for the government.
2) Understand the persecutions associated with a PII Spillage.
3) Understand Personally Identifiable Information (PII) Security Controls.
4) Understand the key Artifacts required to ensure compliance with the requirements set-forth by the various laws and standards impacting PII.

Copyright CyberAdeptness LLC

SCOPE

The scope of this presentation applies to, but is not limited to, the following:

1) Personnel Responsible for Handling Enterprise Level PII Information, including the HR Department.
2) Personnel Responsible for developing and managing systems that handles PII Level Data at the System Level.
3) Personnel Responsible for performing Personnel Background Check Investigations.
4) Personnel Responsible for managing Enterprise Level Incident Response Monitoring and Forensic Investigations.
5) Personnel Responsible for General User and Role Base Training Modules associated with handling and reporting PII Spillage concerns.

Copyright CyberAdeptness LLC

WHAT IS PII

The term “PII,” as defined in OMB Memorandum M-07-1616 refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual.

Copyright CyberAdeptness LLC

WHAT TYPE OF DATA IS CONSIDERED PII

- Social Security #
- Background Check Info
- Drivers License
- Passport Info
- Biometric Data
- Personal Home Address
- Medical Records
- Credit Cards
- Financial Info
- Immigration Data
- Relatives Info
- Full Name
- Bank Account
- Birth Certificate
- Personal Phone Numbers

NOTE: A mix of any of the above leading to an easy identification of an individual can lead to a PII Spillage.

Copyright CyberAdeptness LLC

WHAT ISN'T SENSITIVE PII DATA

- Individuals Name
- Individuals Title
- Work Phone #
- Work Address
- Court Records
- Legal Matters
- Driving Records
- Real Estate Transactions
- Civil and Traffic Records
- Trademarks and Patents
- Social Media Public Data
- Work E-mail

NOTE: Anything deemed PUBLIC data by the Government, State, and Local Agencies and/or is made public by the individual itself on a public forum is no longer considered sensitive data. However, mixing any of the above with what is deemed PII data can indeed lead to a PII Spillage.

Copyright CyberAdeptness LLC

IS ALL PII DATA PROTECTED

NOT ALL PII DATA IS PROTECTED- The final determination lies on the uniqueness of each individual agency and/or organization as they are responsible for clearly delineating which type of PII Data they deem protected based on their unique mission and objectives. Publicly available data made available by the individual within social media platform is not protected.

In some instances, the sensitivity level of the data is highly dependent on the type of data attached to such PII Data and whether such data can lead to harm if disclosed. The correct process to determine the level of protection required entails a ***PII Level Assessment*** which in turn determines the risk associated with such PII Data and any other associated data tied to it.

Copyright CyberAdeptness LLC

PII Data Handling

Overview of key items

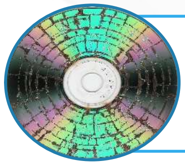
HOW SHALL PII DATA BE HANDLE

DIGITAL and Non-DIGITAL DATA should be...

Encrypted or Shredded

Restricted from View
By unauthorized users

Stored in a
Locked Box



Sanitized Properly
After Spillage

Available as a
Need-To-Know Basis

Audited
Continuously

Handled with Care

Approved for Use by
the individuals impacted

Copyright CyberAdeptness LLC

WHY SHOULD PII BE PROTECTED

DIGITAL and Non-DIGITAL DATA should be protected because…

It could lead to Identity Theft

It could lead to Physical Harm

It could lead to Embarrassment

It could lead to Hefty Fines or Prison

It could lead to Mistrust and Fraud

It could lead to Business Reputation Damage

It could lead to Harassment

It could lead to Theft of Trade Secrets

Copyright CyberAdeptness LLC

PII Security Controls NIST SP 800-53B v5

Overview of key items

WHAT ARE PII CONTROLS

Privacy controls are an administrative, technical, or physical safeguard employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.

This controls set the baseline for agencies and federal government contractors to protect personal data from access by unauthorized individuals.

Copyright CyberAdeptness LLC

ENTERPRISE LEVEL PII CONTROLS

Implemented by:

O > Organization (19)
S > System (2)

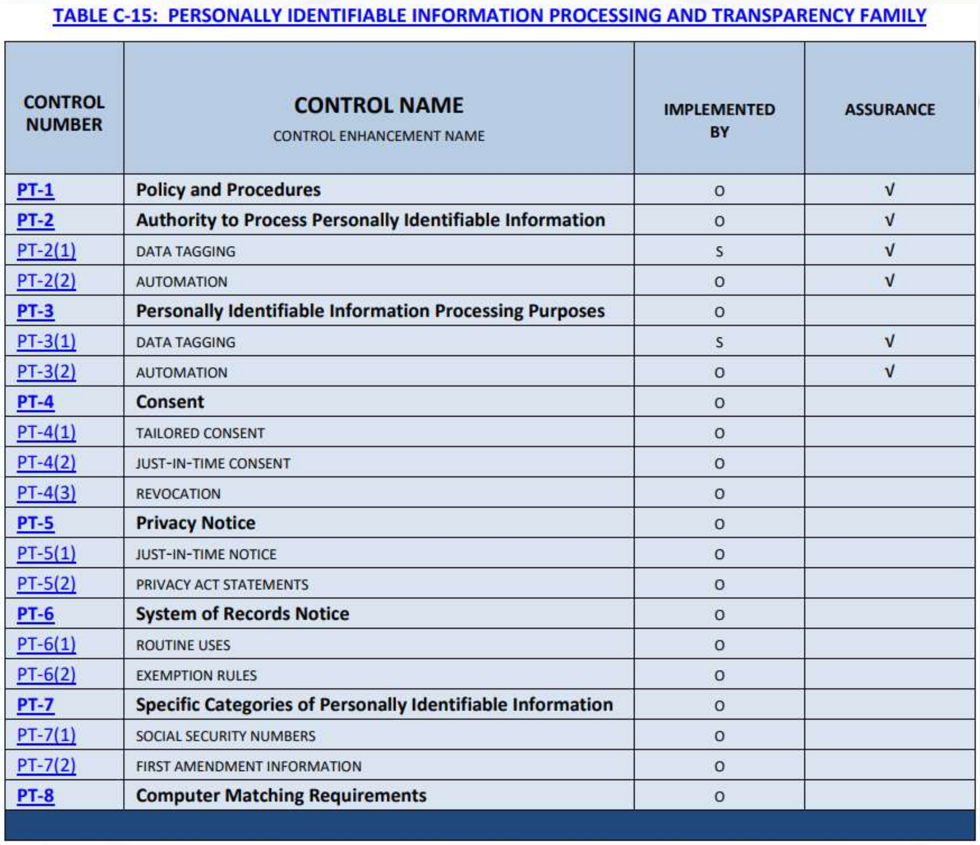


TABLE C-15: PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	IMPLEMENTED BY	ASSURANCE
PT-1	**Policy and Procedures**	O	√
PT-2	**Authority to Process Personally Identifiable Information**	O	√
PT-2(1)	DATA TAGGING	S	√
PT-2(2)	AUTOMATION	O	√
PT-3	**Personally Identifiable Information Processing Purposes**	O	
PT-3(1)	DATA TAGGING	S	√
PT-3(2)	AUTOMATION	O	√
PT-4	**Consent**	O	
PT-4(1)	TAILORED CONSENT	O	
PT-4(2)	JUST-IN-TIME CONSENT	O	
PT-4(3)	REVOCATION	O	
PT-5	**Privacy Notice**	O	
PT-5(1)	JUST-IN-TIME NOTICE	O	
PT-5(2)	PRIVACY ACT STATEMENTS	O	
PT-6	**System of Records Notice**	O	
PT-6(1)	ROUTINE USES	O	
PT-6(2)	EXEMPTION RULES	O	
PT-7	**Specific Categories of Personally Identifiable Information**	O	
PT-7(1)	SOCIAL SECURITY NUMBERS	O	
PT-7(2)	FIRST AMENDMENT INFORMATION	O	
PT-8	**Computer Matching Requirements**	O	

Copyright CyberAdeptness LLC

WHAT IS THE SECURITY CATEGORY

Personally Identifiable Information (PII) Controls are Organizational Level Controls and therefore they must be applied and enforced at the Enterprise Level across the board. Security Category restrictions tied to LOW,MOD, HIGH do not apply to this controls.

While there’s a few that are tied to the system level, applicability must encompass every aspect of the organization, not just the system level data, and every system that handles, stores, transports, or process PII data whether it is bound to a particular system or an enterprise level process.

This means that organizational level PII data handle by the organization as part of their HR Department also falls within the policies and procedures evaluated during a security assessment process.

Copyright CyberAdeptness LLC

HOW SHOULD PII CONTROLS BE SELECTED

- Organizations should conduct a Privacy Risk Assessment to determine the nature of the PII processing and its impact on individuals to guide the tailoring of the privacy control baseline based on the organizations mission and objectives.
- Organizations must consider the nature of the PII being processed by the organization and its impact on individuals in order to guide tailoring of the control baselines.
- The baseline provided can be augmented or further detailed by the organization by incorporating additional sector-specific guidance and/or international level guidance that may be impacting the organization.
- Federal Agencies and contractors handling federal data must consider the applicability of OMB A-130 guidance when tailoring the controls.

Copyright CyberAdeptness LLC

DOES THE ASSESSMENT FOCUS ON SYSTEM SPECIFIC PII DATA

NO

The PII Security Assessment process includes both Organizational Level Policies and system level measures applied to protect the PII Data.

If there’s a PII Spillage while the organization is undergoing a security assessment process, it must be reported as a failure to the organization’s Enterprise Level Policies and Procedures. Failures within the PII Controls Families are not just tied to a system as many individuals wish to portray; they are tied to the organization as a whole.

Artifacts

Overview of key items

WHAT ARE THE KEY ARTIFACTS

- PII Policy
- PII Procedures
- PII Spillage Plan
- PII Training
- PII Incident Response
- System Of Record Notice

Copyright CyberAdeptness LLC

WHAT SHOULD THE PII POLICY INCLUDE

The Policy should include:

- Purpose;
- Scope;
- Roles and Responsibilities;
- Management; Commitment;
- Coordination among; organizational entities;
- Compliance; and
- List of applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

To ensure the policy is developed accordingly, the organization should:

- Designate an *[Assignment: organization-defined official]* to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy;
- Review and update the current personally identifiable information processing and transparency Policy *[Assignment: organization-defined frequency] and following [Assignment: organization-defined events]*

Copyright CyberAdeptness LLC

WHAT SHOULD THE PII PROCEDURES ADDRESS

The Procedures should:

- facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;
- Clearly incorporate step-by-step instructions on how PII data is to be examine forensically, sanitized, and handled when it’s uploaded to a 3rd Party Service Provider for which the organization has minimum or no control.

To ensure the procedures are developed accordingly, the organization should:

- Designate an *[Assignment: organization-defined official]* to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency procedures;
- Review and update the current personally identifiable information processing and transparency Procedures *[Assignment: organization-defined frequency] and following [Assignment: organization-defined events]*

WHAT SHOULD THE PII SPILLAGE PLAN INCLUDE

The PII Spillage Plan should:

- Clearly delineate the roles and responsibilities of those responsible for handling a PII Spillage;
- Clearly delineate the chain of command and reporting mechanisms to be used for reporting;
- Clearly delineate how forensic data is to be handled;
- Clearly delineate how the data impacted will be sanitized- whether it is hosted within internal systems and/or an external 3rd Party Service Provider.
- Clearly delineate the controls impacted by a PII Spillage.

To ensure the procedures are developed accordingly, the organization should:

- Designate an *[Assignment: organization-defined official]* to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency procedures;
- Review and update the current personally identifiable information processing and transparency PII Spillage Plan *[Assignment: organization-defined frequency] and following [Assignment: organization-defined events] or soon after an incident takes place.*

Copyright CyberAdeptness LLC

WHAT SHOULD THE PII TRAINING INCORPORATE

The PII Training should:

- Be Molded to the various roles associated with PII data handling;
- Clearly delineate the organizations policies and procedures;
- Clearly delineate the correct manner of handling PII data;
- Clearly delineate the step-by-step process individuals should take to report a PII Spillage;
- Clearly delineate or ping-point the chain of command to be followed based on the roles impacted by the training;
- Clearly delineate the controls required to protect PII data.

To ensure the procedures are developed accordingly, the organization should:

- Designate an *[Assignment: organization-defined official]* to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency training modules;
- Review and update the current personally identifiable information processing and transparency Training modules *[Assignment: organization-defined frequency] and following [Assignment: organization-defined events] or soon after policies and procedures are updated.*

Copyright CyberAdeptness LLC

WHAT SHOULD THE PII INCIDENT RESPONSE PLAN INCLUDE

The PII Incident Response Plan should:

- Clearly delineate the Roles and Responsibilities of those responsible for handling a PII Incident;
- Clearly delineate how those involved must handle PII Spillage incidents;
- Clearly delineate the step-by-step procedures on how the team must coordinate with other teams and management;
- Clearly delineate how management should handled the consumers impacted in the process and the media;
- Clearly delineate the approval process required before releasing details to the public.

To ensure the procedures are developed accordingly, the organization should:

- Designate an *[Assignment: organization-defined official]* to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency training modules;
- Review and update the current personally identifiable information processing and transparency Incident Response Plan *[Assignment: organization-defined frequency] and following [Assignment: organization-defined events] or soon after policies and procedures are updated.*

Copyright CyberAdeptness LLC

Key Role

Overview of key items

Copyright CyberAdeptness LLC

SENIOR AGENCY OFFICIAL FOR PRIVACY (SAOP)

The term “Senior Agency Official for Privacy” means the senior official, designated by the head of each agency, who has:

- agency-wide responsibility for privacy, including implementation of privacy protections;
- compliance with Federal laws, regulations, and policies relating to privacy;
- management of privacy risks at the agency; and
- a central policy-making role in the agency’s development and evaluation of legislative, regulatory, and other policy proposals.

Copyright CyberAdeptness LLC

WHAT ARE THE RESPONSIBILITIES

The Senior Agency Official for Privacy shall…

- Have access to a complete and accurate list of all of the agency's contracts involving information that identifies and is about individuals;
- shall establish a process to ensure that the language of each contract is sufficient and that the applicable requirements in the Privacy Act and OMB policies are enforceable on the contractor and its employees consistent with the agency's authority.
- Shall oversee all ongoing activities related to the development, implementation, and maintenance of the organization's privacy policies following applicable federal and state laws. B
- Build a strategic and comprehensive privacy program that defines, develops, maintains, and implements policies and processes that enable consistent, effective privacy practices that minimize risk and ensure the confidentiality of protected information, paper and/or electronic, across all media types. Ensures privacy forms, policies, standards, and procedures are up-to-date
- Works with senior organization management, security, and corporate compliance officer to establish governance for the privacy program
- Serves in a leadership role for privacy compliance
- Collaborate with the information security officer to ensure alignment between security and privacy compliance programs, including policies, practices, investigations, and acts as a liaison to the information systems department
- Performs or oversees initial and periodic information privacy risk assessment/analysis, mitigation, and remediation

Copyright CyberAdeptness LLC

WHAT ARE THE RESPONSIBILITIES (CONT.)

- Establishes, with the information security officer, an ongoing process to track, investigate, and report inappropriate access and disclosure of protected information. Monitor patterns of improper access and/or disclosure of protected information
- Develops, delivers, and oversees initial and ongoing privacy training to the workforce
- Works cooperatively with the information management director and other applicable organization units in overseeing customer rights to inspect, amend, and restrict access to protected information when appropriate
- Manages all required breach determination and notification processes under applicable State breach rules and requirements
- Establishes and administers a process for investigating and acting on privacy and security complaints
- Maintains current knowledge of applicable federal and state privacy laws and accreditation standards
- Works with organization administration, legal counsel, and other relevant parties to represent the organization's information and interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standards
- Serves as information privacy resource to the organization regarding the release of information and all departments for all privacy-related issues

Copyright CyberAdeptness LLC

PII Assessment

Overview of key items

Copyright CyberAdeptness LLC

HOW IS PII ASSESSED

A PII Assessment can be done either independently and/or as part of a full Security Assessment. Whichever way is performed, the focus lies on how the organization applies the policies and procedures at the Enterprise Level across the organization- not just at the system level. Due to the uniqueness of each individual organization, the process itself differs.

During this process, we focus on…

- Enterprise Level Policies and Procedures
- Enterprise Level Risk Management
- Enterprise Level PII Risk Assessments
- Enterprise Level PII Incident Handling
- Enterprise Level PII Spillage Tracking Records and Lessons Learned

Copyright CyberAdeptness LLC

ANY MITIGATING CONTROLS

PII Controls are tied to management and high-level procedures; however, they rely on other family controls to function properly. That said, when an assessment takes place, we look at how other essential controls are applied. This controls include, but are not limited to, the following:

- Access Control (AC)
- Audit and Accountability (AU)
- Incident Response (IR)
- Risk Assessment (RA)
- Configuration Management (CM)
- Media Protection (MP)
- Program Management (PM)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)

Keep in mind that there are other factors that impact the assessment such as the environment and 3rd Party Service Providers involvement, if applicable.

Copyright CyberAdeptness LLC

Regulations

Overview of key items

Copyright CyberAdeptness LLC

WHAT ARE THE OMB A-130 REQUIREMENTS FOR PII

According ***to Circular No. A-130 Memorandum addressing Management of Federal Information Resources***, Federal Agencies must abide by the following requirements:

- The individual's right to privacy must be protected in Federal Government information activities involving personal information.
- Consider the effects of their actions on the privacy rights of individuals and ensure that appropriate legal and technical safeguards are implemented.
- Provide access to agency records under provisions of the Freedom of Information Act and the Privacy Act, subject to the protections and limitations provided for in these Acts.
- Provide individuals, upon request, access to records about them maintained in Privacy Act systems of records and permit them to amend such records as are in error consistent with the provisions of the Privacy Act.
- Clearly delineate a summary of the security plan from the agency's five-year plan as required by the PRA and Appendix III of this Circular. The plan must demonstrate that IT projects and the EA include security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from National Institute of Standards and Technology (NIST) security guidance.
- Deploy effective security controls and authentication tools consistent with the protection of privacy, such as public-key based digital signatures, for those systems that promote or permit public access.
- Review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance, with respect to privacy and security, with the Privacy Act, the Freedom of Information Act, the Computer Security Act, the GPEA, and related statutes.

OMB Circular A-130 outlines privacy requirements that apply to the information system development life cycle. Because all information in systems of records is part of one or more information systems, many of the requirements in Circular A-130 apply to systems of records.

For example, agencies are required to select, implement, and assess privacy controls and develop privacy plans for information systems.

Copyright CyberAdeptness LLC

WHAT ARE THE OMB A-108 REQUIREMENTS FOR PII

According ***to Circular No. A-108 Memorandum addressing Maintenance of Records about Individuals***, Federal Agencies must abide by the following requirements:

1) The Privacy Act requires agencies to publish a separate SORN for each system of records. Before developing a SORN, agencies shall carefully consider the proper scope of the system of records. Agencies have discretion in determining what constitutes a system of records for purposes of preparing a notice.
2) Agencies shall publish notice of any new or significantly modified routine uses sufficiently in advance of the proposed effective date of the routine uses to permit time for the public to comment and for the agency to review those comments.
3) Agencies shall draft SORNs in plain language with an appropriate level of detail to ensure that the public is properly informed about the character of the system of records.
4) Agencies shall consult the Office of the Federal Register's Document Drafting Handbook for general guidance on drafting Federal Register notices.
5) Agencies shall consider whether a single SORN or multiple SORNs would provide the best notice to individuals regarding how and where they may request access to their records maintained in the system(s) and would allow the agency to most effectively respond to such requests.
6) Agencies shall design their procurement practices to ensure that all contracts that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of information that identifies and is about individuals are reviewed and approved by the Senior Agency Official for Privacy before award to help evaluate whether a system of records will be established and, if so, to include appropriate clauses in the contract.

..

On July 1, 1975, OMB issued OMB Circular No. A-108, Responsibilities for the Maintenance of Records About Individuals. On September 30, 1975, OMB issued a supplement to Circular A-108 providing expanded guidance on the reporting requirements of the Privacy Act.

This additional guidance on reporting requirements, which was subsequently updated, superseded the preliminary guidance on reporting requirements contained in the Privacy Act Guidelines

Copyright CyberAdeptness LLC

WHAT IS A SORN

The term “system of records notice” (SORN) means the notice(s) published by an agency in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system. The Privacy Act requires agencies to publish a SORN in the Federal Register describing the existence and character of a new or modified system of records.

A SORN may be comprised of a single Federal Register notice addressing all of the required elements that describe the current system of records, or it may be comprised of multiple Federal Register notices that together address all of the required elements. The requirement for agencies to publish a SORN allows the Federal Government to accomplish one of the basic objectives of the Privacy Act – fostering agency accountability through public notice.

The SORN must:

- Clearly delineate the purpose(s) of the system;
- Clearly delineate the categories of records maintained in the system;
- Clearly delineate the categories of individuals about whom records are maintained;
- Clearly delineate the routine uses to which the records are subject; and
- Clearly delineate additional details about the system.

To ensure the SORN is developed and maintained properly, the organization should:

- Identify all systems impacted by the Privacy Act and associated standards.
- Perform a PII Security Assessment on all systems being developed to determine the risk level required to populate the SORN data.
- Review the SORNs annually and/or whenever major changes take place.

NOTE: The Privacy Act requires agencies to publish any new or modified routine use at least 30 days before the effective date of the routine use.

An agency shall not disclose any records pursuant to a new or modified routine use until after the 30-day comment period has ended and the agency has considered any comments from the public and determined that no further modifications are necessary.

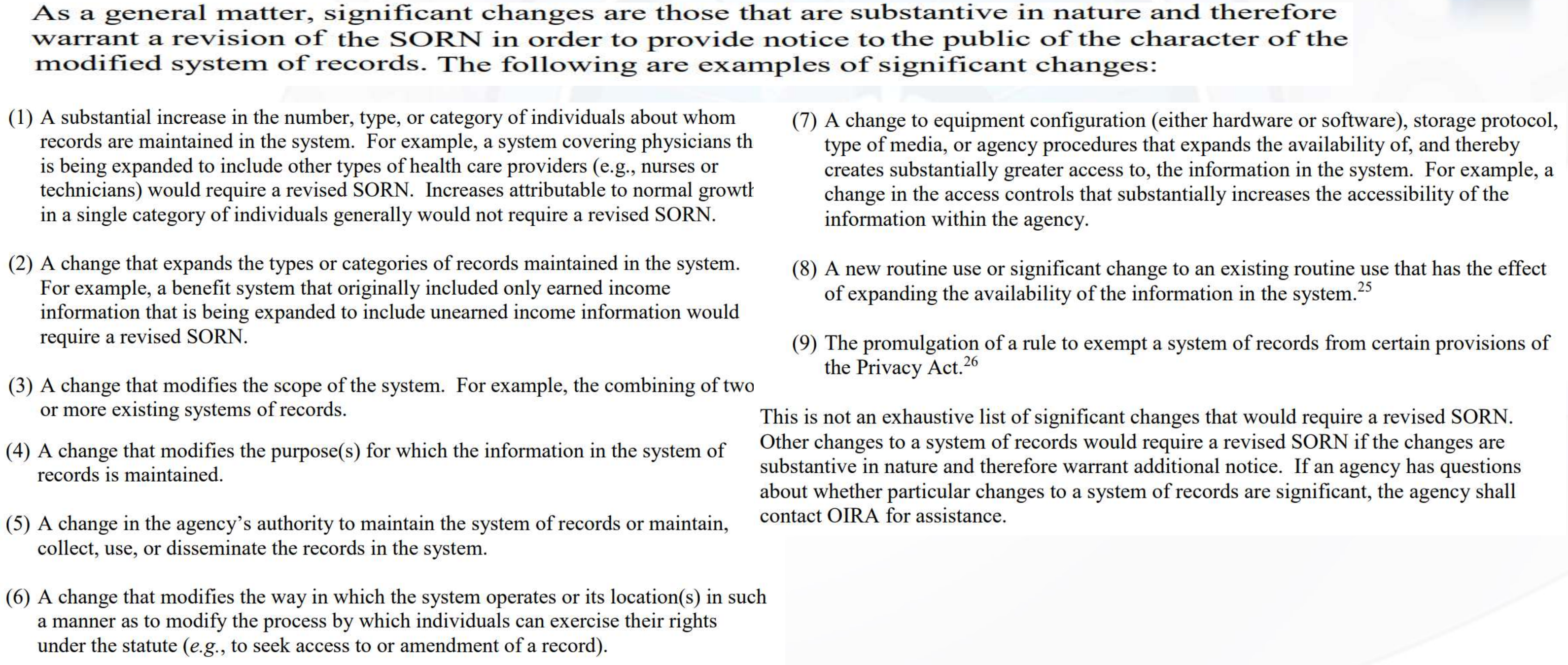
Copyright CyberAdeptness LLC

WHEN IS A SORN REQUIRED

A SORN is required when…

There's a NEW SYSTEM handling PII

There's MAJOR CHANGES to an existing SORN



As a general matter, significant changes are those that are substantive in nature and therefore warrant a revision of the SORN in order to provide notice to the public of the character of the modified system of records. The following are examples of significant changes:

(1) A substantial increase in the number, type, or category of individuals about whom records are maintained in the system. For example, a system covering physicians th is being expanded to include other types of health care providers (e.g., nurses or technicians) would require a revised SORN. Increases attributable to normal growtl in a single category of individuals generally would not require a revised SORN.

(2) A change that expands the types or categories of records maintained in the system. For example, a benefit system that originally included only earned income information that is being expanded to include unearned income information would require a revised SORN.

(3) A change that modifies the scope of the system. For example, the combining of two or more existing systems of records.

(4) A change that modifies the purpose(s) for which the information in the system of records is maintained.

(5) A change in the agency's authority to maintain the system of records or maintain, collect, use, or disseminate the records in the system.

(6) A change that modifies the way in which the system operates or its location(s) in such a manner as to modify the process by which individuals can exercise their rights under the statute (*e.g.*, to seek access to or amendment of a record).

(7) A change to equipment configuration (either hardware or software), storage protocol, type of media, or agency procedures that expands the availability of, and thereby creates substantially greater access to, the information in the system. For example, a change in the access controls that substantially increases the accessibility of the information within the agency.

(8) A new routine use or significant change to an existing routine use that has the effect of expanding the availability of the information in the system.[25]

(9) The promulgation of a rule to exempt a system of records from certain provisions of the Privacy Act.[26]

This is not an exhaustive list of significant changes that would require a revised SORN. Other changes to a system of records would require a revised SORN if the changes are substantive in nature and therefore warrant additional notice. If an agency has questions about whether particular changes to a system of records are significant, the agency shall contact OIRA for assistance.

Legal Persecutions

For Mishandling PII Information

WHAT ARE THE PERSECUTIONS FOR BREAKING THE LAW

Hefty Fines

Job Loss

Lawsuits

Reputation Damage

Business Reputation Loss

Business Financial Loss

Copyright CyberAdeptness LLC

Send them to
info@cyberadeptness.com

Need Help?

We have over 20+ years of combined experience in the field and a unique process to streamline the requirements.

Contact us today to schedule a meeting and determine how we may be of help to your organization. Our processes are flexible to accommodate compliance needs, regardless of sector (i.e., Healthcare, Finance, Law, Education, etc.).

Copyright CyberAdeptness LLC

References

❑ **M-07-16 Memorandum For the Heads of Executive Departments and Agencies >** https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

❑ **Privacy Act of 1974 (Privacy Act) >** https://www.archives.gov/about/laws/privacy-act-1974.html

❑ **NIST SP 800-53B v5 >** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

❑ **NIST SP 800-53 v5 >** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

❑ **OMB A-130 >** https://www.cio.gov/policies-and-priorities/circular-a-130/

❑ **OMB A-108 >** https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_circular_a-108.pdf