Air Force

PII Confidentiality Impact Level (PCIL) Categorization Worksheet

Air Force Family Integrated Results & Statisical Tracking

AFFIRST

System Version 4.2

Change History

Version	Date of change	Author(s)	Description of Change
1.1 USAF	FEBRUARY 2018	USAF (L. White)	Template approved
Version of PCIL		Author's Name	Provide description of change
Version of PCIL		Author's Name	Provide description of change
Version of PCIL		Author's Name	Provide description of change
Version of PCIL		Author's Name	Provide description of change

1. Overview

Identifying the system's Personally Identifiable Information (PII) confidentiality impact level (PCIL, pronounced like "pickle") value is a follow-on step to the information system provisional security categorization step. Note that although the PII confidentiality impact level sounds similar, it is different from, and does not equate to, the impact values for the security objectives of confidentiality, integrity, and availability for the system overall, which are used to determine the security control baselines in CNSSI No. 1253. Once the PII confidentiality impact level value is selected, it should be used to select the appropriate Privacy Overlay – whose controls are added to the previously selected security control baseline.

1.1 Purpose

To assist the AFFIRST team in conducting the analysis associated with determining the PII confidentiality impact value for the Privacy Overlay.

1.2 Scope

This work sheet is specific to AFFIRST and the associated Privacy Overlay.

1.3 Instruction

Per DoDI 8510.01, Reference (e) is used to conduct the Privacy Overlay categorization analysis for the information system. Reference (e) will further reference (NIST SP 800-122, FIPS 199, and NIST SP 800-37).

1.4 Four Key Questions

The PII Confidentiality Impact Level analysis conducted IAW reference (e) will answer four questions:

1. *Does the information system collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?*
2. *Does Exception of the Business Rolodex Information apply?*[1]
3. *Is the PII confidentiality impact level low, moderate, or high?*
4. *Is your organization a covered entity or business associate under HIPAA?*

Once these four questions have been answered, the information system security manager will use the PII confidentiality impact level (**PCIL** – pronounced like "pickle") value to select the appropriate Privacy Overlay(s) (e.g., low, moderate, high, and/or PHI).

Per Reference (e), "Organizations should encourage close coordination among their chief privacy officers, senior agency officials for privacy, chief information officers, chief information security officers, and legal counsel when addressing issues related to PII."

- ***The PCIL analysis process begins in Section 2 (see below).***
- ***Once the PCIL analysis has been completed, the Information System Security Manager and Program Manager should review and sign the worksheet at Appendix B, and forward the worksheet to the Privacy Officer for review and signature.***

[1] See section 2.2 below.

- ***The Privacy Officer will provide a signed copy of the worksheet that will accompany the DD Form 2930 (Privacy Impact Assessment), provided by the ISSM for the information system.***

2. Analyze PII Data and Determine PCIL

2.1 Does the information system contain, process, or transact PII?

PII is defined in Reference (e) as (i) data elements which alone can distinguish or trace an individual's identity, i.e., unique identifiers; (ii) non-PII that becomes PII when it identifies an individual in aggregate, i.e., compilation effect; and (iii) non-PII that becomes PII when combined with a unique identifier or data elements that have aggregated to become PII, i.e., by association.

Given the definition provided, determine if the applicable system contains PII. In order to make this determination, consider the Privacy Impact Assessment (PIA), the system data elements/dictionary, mission description, and system data description. All of these items should be discussed in Reference (i).

*Note: Historical data maintained within the system still requires PII protections and should be considered in the analysis.

(●) YES ( ) NO

- ***If the response selected for item 2.1 is, "NO," then sign at Appendix B.***
- ***If the response selected for item 2.1 is, "YES," then continue to item 2.2.***

2.2 Use the space below to identify the types of PII and data elements contained in, processed by, or transacted through the information system:

The PII in this system consists of SSN (not a required field and all but last 4 masked in system), DOD ID, Full Name, Rank, Military Organization, DoB, Marital Status, Address, Phone Number, Email Address and Gender.

2.3 Estimate the number of records containing PII:

This system contains approximately one million records (system has been online since 2004).

2.4 Define the user community:

AFFIRST is used by all Active Duty, Guard and Reserve Airman & Family Readiness Centers (A&FRC) staffs and Higher Head Quarters (HHQ) counterparts to document services provided to A&FRC customers. Only the aforementiond categories of individuals have assess to the system via an approved user account that requires a two factor Common Access Card (CAC) login. Customers do not access the system.

2.5 Does the Business Rolodex Information Exception apply?

*Refer to **Appendix C** or to Reference (e), section 2.4, pages 9-10, to determine if the PII within the applicable system meets the "Exception of Business Rolodex Information."*

○ YES. ROLODEX APPLIES ◉ NO. ROLODEX does NOT apply

If Yes, provide explanation:

Do not beleive ROLODEX applies to AFFIRST.

- ***If the response selected for item 2.5 is "YES," then sign at Appendix B.***
- ***If the response selected for item 2.5 is "NO", continue to Section 2.6.***

2.6 Determine the PII confidentiality impact level (PCIL)

The PII confidentiality impact level (PCIL) in NIST SP 800-122 — low, moderate, or high — is based on a combination of the FIPS 199 impact values and six factors for determining the harm[2] (*see* Table 2 below) that could result to the subject individuals, the organization, or both, if PII were inappropriately accessed, used, or disclosed.[3]

The Privacy Overlay (Reference (e)) references FIPS 199 (Reference (d)) for a definition of the impact levels and NIST SP 800-122 (Reference (f)) for six (6) factors that determine the harm that could result to individuals, the organization, or both.

[2] NIST SP 800-122, Section 3.1, "For the purposes of this document, *harm* means any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging). Examples of types of harm to individuals include, but are not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of confidentiality of PII maintained by the organization, including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and legal liability."

[3] NIST SP 800-122, Section 3.2, discusses the use of six factors to determine impact levels and the freedom of agencies to determine the most relevant factors, including extending the six factors when appropriate. The six factors include identifiability, quantity of PII, data field sensitivity, context of use, obligation to protect confidentiality, and access to and location of PII (see Table 2 of the Privacy Overlays for illustrative examples of these six factors for each PII confidentiality impact level). NIST SP 800-122 leaves it to the organization's discretion to determine whether additional factors should be considered beyond the six defined by NIST. NIST also notes the importance of considering the relevant factors together as the impact levels of each factor may differ.

In order to determine the PII confidentiality impact level, the impact levels from Reference (d) and the 6 factors from Reference (f) should be used together using a "Balanced Approach." The "Balanced Approach" considers all inputs as an average. It is a best judgment standard where the analyst considers the values and various weights of the individual components. This "Balanced Approach" takes all factors into consideration to determine the PII confidentiality impact level.

2.6.1 STEP 1. REVIEW THE FIPS 199 IMPACT VALUE FOR EACH OF THE SIX FACTORS.

- ***Carefully read the definitions of each impact value in Table 1 (below). Use these definitions, as tailored below in Step 2, to determine the impact value for each of the six factors from NIST SP 800-122.***

Table 1: FIPS 199 Potential Impact Values as Incorporated in NIST SP 800-122

Potential Impact Value	Type of adverse effect on organizational operations, organizational assets, or individuals	Expected adverse effect of the loss of confidentiality, integrity, or availability on organizational operations, organizational assets, or individuals
LOW	Limited	1. cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; 2. result in minor damage to organizational assets; 3. result in minor financial loss; or 4. result in minor harm to individuals.
MODERATE	Serious	1. cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2. result in significant damage to organizational assets; 3. result in significant financial loss; or 4. result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
HIGH	Severe or catastrophic	1. cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; 2. result in major damage to organizational assets; 3. result in major financial loss; or 4. result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

2.6.2 STEP 2. USING THE GUIDANCE PROVIDED BELOW, DETERMINE THE IMPACT VALUE FOR EACH OF THE SIX (6) FACTORS FROM NIST SP 800-122

FACTOR 1 – IDENTIFIABILITY

NIST SP 800-122	NIST SP 800-122 PII Confidentiality Impact levels[4]

4. Note: the descriptions given in the Low, Moderate, and High cells are examples. They are for illustrative purposes and provided to clarify both the more general descriptions in Table 1 and the six factors from NIST SP 800-122; each instance of PII is different, and each organization has a unique set of requirements and different missions to consider. Refer directly to NIST SP 800-122 section 3.2 for a more complete description of the 6 factors.

Factors	Low	Moderate	High
Identifiability	Data elements are not directly identifiable alone but may indirectly identify individuals or significantly narrow large datasets.	Combined data elements uniquely and directly identify individuals.	Individual data elements directly identifying unique individuals.

Factor 1. Select Identifiability impact value:

☐ LOW ☐ MODERATE ☑ HIGH

Only A&FRC staff with an approved user account that requires a 2 factor Common Access Card (CAC) login have access to this information on a need to know basis in performance of their duties.The SSN can be entered into AFFIRST but it isn't a mandatory fields and all but the last four digits are masked. Working towards eliminating the SSN from the system in the near future.

FACTOR 2 -- QUANTITY OF PII

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact levels[5]		
	Low	Moderate	High
Quantity of PII	A limited number of individuals affected by a loss, theft, or compromise. Limited collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.	A serious or substantial number of individuals affected by loss, theft, or compromise. Serious collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. Aggregation of a serious or substantial amount of data.	A severe or catastrophic number of individuals affected by loss, theft, or compromise. Severe or catastrophic collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. Aggregation of a significantly large amount of data, e.g., "Big Data."

Factor 2. Select Quantity of PII impact value:

☐ LOW ☑ MODERATE ☐ HIGH

Based on the type of information being collected and the fact that not all records have uniques identifiers such as the SSN (not a required field and all but the last four digits are masked). Do not believe the type and amount of data being collected rises to the level of catastrophic impacts.

[5] Ibid

FACTOR 3 - DATA FIELD SENSITIVITY

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact levels[6]		
	Low	Moderate	High
Data Field Sensitivity	Data fields, alone or in combination, have little relevance outside the context.	Data fields, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.	Data fields, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.

Factor 3. <u>Select</u> Data Field Sensitivity impact value:

☐ LOW ☑ MODERATE ☐ HIGH

Based on the type of data captured and the fact no HIPPA or classified data is collected in the system.

FACTOR 4 -- OBLIGATION TO PROTECT CONFIDENTIALITY

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact levels[7]		
	Low	Moderate	High
Obligation to Protect Confidentiality	Government-wide privacy laws, regulations or mandates apply. Violations may result in limited civil penalties.	Role-specific privacy laws, regulations or mandates (e.g., those that cover certain types of healthcare or financial information) apply that add more restrictive requirements to government-wide requirements. Violations	Organization or Mission-specific privacy laws, regulations, mandates, or organizational policy apply that add more restrictive requirements to government-wide or industry-specific requirements. Violations

[6] Ibid

[7] Ibid

		may result in serious civil or criminal penalties.[8]	may result in severe civil or criminal penalties.

Factor 4. Select Obligation to Protect Confidentiality impact value:

☑ LOW ☐ MODERATE ☐ HIGH

The Government-wide privacy laws, regulations or mandates apply to this system. No HIPPA or classified data is collected in the system.

FACTOR 5 -- ACCESS TO AND LOCATION OF PII

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact levels[9]		
	Low	Moderate	High
Access to and Location of PII	Located on computers and other devices on an internal network. Access limited to a small population of the organization's workforce, such as a program or office which owns the information on behalf of the organization. Access only allowed at physical locations owned by the organization (e.g., official offices). Backups are stored at government-owned facilities. PII is not stored or transported off-site by employees or contractors.	Located on computers and other devices on a network controlled by the organization. Access limited to a multiple populations of the organization's workforce beyond the direct program or office that owns the information on behalf of the organization. Access only allowed by organization-owned equipment outside of the physical locations owned by the organization only with a secured connection (e.g., virtual private network (VPN)). Backups are stored at contractor-owned facilities.	Located on computers and other devices on a network not controlled by the organization or on mobile devices or storage media. Access open to the organization's entire workforce. Remote access allowed by equipment owned by others (e.g., personal mobile devices). Information can be stored on equipment owned by others (e.g., personal USB drive).

Factor 5. Select Access to and Location of PII impact value:

[8] The Privacy Act of 1974 contains both civil and criminal penalties.

[9] Ibid

☐ LOW ☑ MODERATE ☐ HIGH

The system is for used by Airman & Family Readiness Center (A&FRC) and requires an approved user account and login with two factor Common Access Card (CAC). AFFIRST is a web-based system and is hosted and maintained in an accredited hosting facility.

FACTOR 6 -- CONTEXT OF USE

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact levels[10]		
	Low	Moderate	High
Context of Use	Disclosure of the act of collecting, and using the PII, or the PII itself is unlikely to result in limited harm to the individual or organization such as name, address, and phone numbers of a list of people who subscribe to a general-interest newsletter.	Disclosure of the act of collecting, and using the PII, or the PII itself may result in serious harm to the individual or organization such as name, address, and phone numbers of a list of people who have filed for retirement benefits.	Disclosure of the act of collecting, and using the PII, or the PII itself is likely to result in severe or catastrophic harm to the individual or organization such as name, address, and phone numbers of a list of people who work undercover in law enforcement.

Factor 6. <u>Select</u> Context of Use impact value:

☐ LOW ☑ MODERATE ☐ HIGH

The system dosen't divulage that a customer works in udercover law unforecement or other similar fields.

2.6.3 STEP 3. DETERMINE PII CONFIDENTIALITY IMPACT LEVEL (PCIL) VALUE

- ***Use the following table to roll up the previous answers from Factors 1 through 6. Enter an "X" in the Low, Moderate, or High column for each row. Use these values to determine the PII Confidentiality impact level (PCIL) value.***

Factor	Impact Value
Identifiability	High
Quantity of PII	Moderate

[10] Ibid

Data Field Sensitivity	Moderate
Obligation to Protect Confidentiality	Low
Access to and Location of PII	Moderate
Context of Use	Moderate

2.6.4 STEP 4. SELECT PII CONFIDENTIALITY IMPACT LEVEL (PCIL) VALUE:

OVERALL PCIL VALUE	MODERATE

- ***Justify your selection of the overall*** PII Confidentiality impact level ***(PCIL) value***. Take into consideration the FIPS 199 impact values from Table 1 (above) and the six factors from NIST SP 800-122. Use the "Balanced Approach" described in Section 2.6.

Selected Moderate based on the fact there was one 1 high, 4 mediums and 1 Low categorization. AFFIRST does store customer demographic data and infomation on services provided to customers by the Airman & Family Readiness Center (A&FRC) staff. Do not feel collected infomation rasies to the High (Severe or Catastrphic) expected adverse affect conditions...loss of life, major damage to

2.7 Is your organization a covered entity or business associate under HIPAA?

2.7.1 Select Organization HIPAA Status:

○ COVERED ENTITY ○ BUSINESS ASSOCIATE ◉ N/A

Refer to the Privacy Overlay for a complete description. Depending upon the types of information contained in it and who uses the information system, you may have to apply the PHI Overlay as well. Essentially, if your system could contain PHI, you must contact the Air Force Office of General Counsel to obtain an opinion.

- ***If your organization is a covered entity or business associate and your system contains PHI, then the PHI Overlay applies as well.***

Appendix A — References

a. DODI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 10 November 2015

b. CNSSI 1253, Security Categorization and Control Selection for National Security Systems, 27 March 2014

c. NIST SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010

d. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004

e. CNSSI 1253, Appendix F, Attachment 6, Privacy Overlays

f. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010

g. NIST SP 800-60, Vol I, Guide for Mapping Types of Information and Information Systems to Security Categories

h. NIST SP 800-60, Vol II, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

i. DoD DD Form 2930, Privacy Impact Analysis

j. Applicable Privacy Act System of Records Notice, http://dpcld.defense.gov/Privacy/SORNs.aspx

k. OMB Circular A-130, “Managing Information as a Strategic Resource,” 07/28/2016, 81 FR 49689

l. OMB Circular A-108, “Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act,” 12/23/2016, 81 FR 94424

Appendix B — Signatures

Information System Security Manager

DAVID R. BELVAL, GS-13, DAF
Information System Security Manager
AFPC/DFCC

Program Manager

PATRICK I. WOODWORTH, GS-12, DAF
Data & Resource Manager
AFPC/DPFF

Air Force Privacy Officer

LaDONNE L. WHITE, DAFC,
Air Force Privacy and Civil Liberties Officer
SAF/CIO A6XA

Appendix C — Definitions

The "Rolodex Exception"

OMB M-07-16, Footnote 6, establishes the flexibility for an organization to determine the sensitivity of its PII in context using a best judgment standard. The example provided in footnote 6 addresses an office rolodex and recognizes the low sensitivity of business contact information used in the limited context of contacting an individual through the normal course of a business interaction. The Privacy Overlays refers to this example from OMB M-07-16, Footnote 6, as the "Rolodex Exception." PII meeting the "Rolodex Exception" typically presents a very low risk to privacy for the individual or the organization and will not trigger implementation of the low, moderate, or high Privacy Overlays for a system containing only this type of information. Consistent with NIST and CNSS tailoring guidance, the "Rolodex Exception" is a scoping decision that, when applicable, helps organizations avoid unnecessary expenditures of resources based on a risk determination for this limited subset of PII.

For the purposes of implementing the low, moderate, and high Privacy Overlays, PII that may be included in this "Rolodex Exception" is limited to the following business contact information:

- Name (full or partial)
- Business street address
- Business phone numbers, including fax
- Business e-mail addresses
- Business organization

An example of an information system which may meet the parameters of the Rolodex Exception include office rosters that contain only business contact information.

Before choosing to apply the Rolodex Exception, an organization must consider the sensitivity of the PII based on the complete context in which it appears. Business contact information alone can be sensitive under certain circumstances, such as in association with a tax return or on a list of individuals under investigation for fraud, waste, and abuse. Consider, also, whether the contact information includes a blend of business and personal information (e.g., a business phone number may be a personal device, or a business address may be a residential address of a home office). If, after exploring contextual considerations, the organization determines that a system's use of the business contact information is limited to business contact purposes, then the organization may apply the Rolodex Exception.

This analysis must include an evaluation of related operational security issues, which are distinct from privacy considerations and may require additional protective measures. Application of this Rolodex Exception is limited to the Privacy Overlays and does not affect applicability of any other statute, regulation, or standard which may require consideration and protection of this type of information in other contexts. For example, consider business contact information which both meets the terms of the Rolodex Exception and appears in a context that has increased classification or operational security sensitivities; the Rolodex Exception may obviate the organization from implementing the Privacy Overlays, but the organization must still meet requirements that are applicable to protect classified information and resolve operational security concerns.