How to Review a Privacy Act System of Records Notice

By Bethanne Barnes and Maya A. Bernstein

apdu
ASSOCIATION of PUBLIC DATA USERS

What is a System of Records Notice?

The Privacy Act of 1974 requires federal agencies to tell the public when they collect personal information that meets certain conditions. They do this by publishing a system of records notice (SORN) for any "system of records" covered by the Act.[1] The SORN serves as a formal statement to the public about:

- **What** records the agency is collecting, about **whom**, and **why**.
- **Who else** outside the agency will see the records, and for what reason.
- **Which** Privacy Act rights are being limited (exemptions).
- **How** individuals can see their own records and request amendments.

Think of a SORN as a public rulebook. Once an agency publishes a SORN in the *Federal Register*, they must follow it.

Why This Guide? Why Should I Review a SORN?

All parties interested in an agency's activities should understand SORNs so they can stay informed and, if they support or oppose proposed changes, know how to submit comments. For example:

- States and grantees may want to know how the federal government uses and discloses the information they report about the individuals they serve.
- Advocacy organizations may want to understand what records an agency collects and shares.
- News organizations may want to learn how information flows among agencies, how agency functions may change, and how to identify relevant documents.
- Individuals may want to find out how they can view and request amendments to their own records.

SORNs provide a window on current and planned agency activities affecting individuals. Understanding the basics of a SORN will help interested parties file useful comments and influence agency actions. This guide helps everyone to understand and evaluate SORNs.

How Do I Use This Guide?

Reviewing a SORN is a technical exercise that is unfamiliar to most people, and your time is likely limited. This guide is designed to help you prioritize:

- **The Big Picture:** This section helps you get your bearings. It also highlights broad issues and cross-cutting questions to watch out for.
- **Section-by-Section Review:** This section gives you a deep dive into each section of the SORN.
- **The SORN Review Checklist (Appendix A):** Think of this as your two-page "cheat sheet," whether you have 30 minutes or three hours to review.

1 For more information about SORNs and Privacy Act requirements, refer to the APDU *Primer on the Privacy Act of 1974* available at https://apdu.org/apdu-in-action/Data-Privacy-Resources/.

Understanding the Layout

This Guide decodes the SORN as published in the *Federal Register*. To do so, it brings together information from multiple official guidance documents, insights from decades of experience reviewing SORNs and working on related issues, and pointers to helpful but non-essential related information and processes. That's a lot to keep straight. This guide assigns specific formatting to help you keep track of these different kinds of information (described below). In addition, SORNs consist of nearly two dozen standardized sections, officially called "elements." Some of these sections only need to be included in the SORN if the SORN is new or if the section is actively being updated. These sections will always appear in the same order (if they appear), and this guide follows that standard order.

BOLD CAPITALS ARE THE NAME OF THE SORN SECTION (Parentheticals next to a title indicate if the section is optional)

Plain text represents a plain language description of what the agency is officially required to include in that section of the SORN. We compiled the requirements from multiple sources, including OMB Guidance and implementing regulations, so you just have to look in one place.

Blue shaded boxes are a distillation of decades of experience reviewing SORNs and give context for that section. We call these "tips." Some tips indicate the relative importance of a given section of the SORN. Others share historical best practices or common practice. Still others explain how these sections relate to other parts of the SORN or other data-related processes. We don't have tips for every section.

- ❑ Yellow shaded boxes list items to check for in your review. They are structured as questions for you to consider as you exercise your own judgement in assessing the SORN's potential strengths and weaknesses.
- ❑ You may want to add items of your own to these lists.
- ❑ We don't have questions for consideration for every section.

Gray boxes contain pointers on how to find other resources related to that section of the SORN. These outside resources usually aren't essential to the review, but you may find them helpful in sorting through tricky questions or putting together a more contextualized understanding of the current SORN. We don't have pointers for every section.

THE BIG PICTURE

A SORN is a legally binding plan for how an ***agency***[2] handles personal information. Navigating a SORN can be a challenge, so this document is here to guide you. This section provides the high-level context you need to structure a review and know what to watch out for.

Structure of the SORN and the *Federal Register* Notice

Before you begin, it is helpful to know some basics about the structure of the SORN.

The SORN is published in a *Federal Register* notice (FRN). While people often call the whole document a "SORN," the FRN is made up of two parts, which are not formally labeled in the *Federal Register*:

- The Preamble: Think of this as an introduction or a cover note. It provides background and explains what the agency *intends* to do, but it is not legally binding going forward. The preamble ends with the **SIGNATURE**.
- The SORN: Begins with **SYSTEM NAME AND NUMBER**. This is the most important part because it is legally binding.

Issued in Washington, DC.

Charles Chalmers,

Deputy General Counsel, Pension Benefit Guaranty Corporation.

Signature:
Ends the Preamble

SYSTEM NAME AND NUMBER:

PBGC-1: Congressional Correspondence.

Beginning of SORN:
Remainder is legally binding

SORN Scope: How Much Is Covered in One Notice?

Agencies have a lot of freedom when they define the scope of a system of records. OMB's guidance instructs agencies to weigh the following five considerations when deciding whether a group of records should be a single system of records or several:

1. The agency's ability to comply with the requirements of the Privacy Act[3] and facilitate the exercise of the rights of individuals.
2. The informative value of the notice (whether a single or multiple SORNs would best inform the public about the existence and use of the system(s)).

2 A Privacy Act agency is a federal executive branch cabinet-level agency (or the highest level of a non-cabinet agency), excluding parts of the Executive Office of the President that are primarily advisory in nature. See 5 U.S.C. § 552a(a)(1) or APDU's *Primer on the Privacy Act of 1974* for a full definition and discussion, available at https://apdu.org/apdu-in-action/data-privacy-resources/.

3 For an overview of the Privacy Act, refer to the APDU *Primer on the Privacy Act of 1974* available at https://apdu.org/apdu-in-action/Data-Privacy-Resources/.

3. The agency's ability to be responsive to individual access requests (whether a single or multiple SORNs would best inform the public about how to request access to their information in the system(s) and allow the agency to respond effectively).
4. The purpose(s) and use(s) of the records, especially whether different groups of records have different routine uses, security requirements, or groups of employees requiring access (even if all records share a common purpose).
5. The cost and convenience to the agency, but only to the extent consistent with the considerations above regarding compliance and individual rights.

> **Tips**
>
> We interpret OMB's guidance to mean that agencies must do two main things:
>
> - **Check for commonalities.** Before combining records into one SORN, an agency should make sure they share the same **AUTHORITIES**, **PURPOSES**, **CATEGORIES OF INDIVIDUALS**, **SAFEGUARDS**, and **ROUTINE USES**.
> - **Put people over paperwork.** Agencies must prioritize your ability to use your privacy rights. They shouldn't bundle records to save themselves time or money if it makes it harder for you to understand the notice or for them to honor your rights.

The Strategy: How to Review Efficiently.

The Section-by-Section Review guide, which begins on page 6, follows the standard *Federal Register* order.

> **Tip**
>
> However, in our experience the most efficient and effective way to review is NOT to read top to bottom. Instead, prioritize based on impact:

High Priority Sections ***If you're short on time, focus on these.***	
PURPOSE	These are the most important and most impactful sections of the SORN. ROUTINE USES and EXEMPTIONS (if claimed) will likely take the most time
CATEGORIES OF INDIVIDUALS	
CATEGORIES OF RECORDS	
ROUTINE USES	
EXEMPTIONS (full review + rule)	
Lower Priority Sections ***If you've got more time, review these.***	
Remainder of the SORN, except for **SUPPLEMENTAL INFORMATION**	Provide context for the high priority sections or important (but usually low risk) procedural information.
SUPPLEMENTAL INFORMATION (the bulk of the preamble)	Always read this last. It describes what the agency thinks it's doing; it is aspirational and not binding.
Repeat ***If you still have time, review the whole thing again.***	
Now that you know more, you may find things that you missed the first time through	

Common Agency Habits that Complicate Review

Agencies often seek to streamline SORNs to save time, be more consistent across the agency, or make them easier to maintain. This can make your review harder. Watch for:

- **The Bundle:** A single notice that lists multiple systems of records rather than separate notices for each. The list will show up in **SYSTEM NAME AND NUMBER**.
- **The Blanket:** The agency publishes a single list of "blanket routine uses" in the FRN. They then apply this list, in whole or in part, to existing and future SORNs.
- **The Fragment:** When updating a SORN, an agency might only publish the specific sections they are changing. They don't include the full, updated document.

Tips

- You can comment if this "streamlining" makes it harder to understand the notice.
- It is possible that a SORN "fragment" won't include all the high priority sections listed above. For example, the agency might only be adding a ***ROUTINE USE*** and doesn't include any of the other sections in the SORN revision. You will have to find the current version of those other sections to view the changes in context.

How to Find a "Clean" Copy

OMB guidance tells agencies to post a "clean," compiled version of their most recent SORNs on their privacy page: **www.[agency].gov/privacy**.

- **If it's there:** Use it! It's much easier than reading fragments.
- **If it's not:** A web search is your best bet.
- **If all else fails:** You will have to build your own copy by looking through the older notices listed in the **HISTORY** section or searching in the *Federal Register* for the SORN number, found in the **SYSTEM NAME AND NUMBER** section.

What Is a Government-wide System of Records?

You may come across a "government-wide" system of records. A government-wide system of records is a "legal fiction" created by OMB that allows one agency (like the Office of Personnel Management) to create a single SORN to cover similar records held by all agencies. These are usually for common things like employee personnel files. Even if the records are physically sitting at different agencies, that one government wide notice applies to all of them.

SECTION BY SECTION REVIEW GUIDE

This part of the guide explains each section of a SORN's *Federal Register* Notice and questions for you to consider. It closes with cross-cutting and pragmatic items.

The Preamble

The Preamble is the "wrapper" for the SORN. It provides context but is **not legally binding** after the comment period closes**.**

NAME OF AGENCY

This should be the Cabinet-level agency or the highest level of any non-cabinet agency. Subagencies may be named, but legal responsibility sits at the top.

> **Tip**
>
> You are unlikely to comment substantively on this section

ACTION

This says whether it is a new SORN or a SORN revision, also known as a modification.

> **Tips**
>
> You are unlikely to comment substantively on this section. If it is a revision, then the FRN might be a "fragment." That is, it may leave out some critical sections of the SORN if they aren't changing. Below, we note the sections that might be missing.

SUMMARY

This should be a plain-language summary of the system of records and the current notice.

> **Tip**
>
> You are unlikely to comment substantively on this section.

DATES

This includes two key dates: 1) the comment deadline, and 2) the effective date for new or modified routine uses, which must be at least 30 calendar days after official publication in the *Federal Register*. Any prior availability of the SORN doesn't alter the 30-day clock.

> **Tip**
>
> Pay attention to the comment deadline because the agency is not required to consider comments submitted after that date.

ADDRESSES

This says how to submit comments on the proposal, including an email address or a website where comments can be submitted electronically.

> **Tips**
>
> Best practice is for the agency to include multiple contact methods, such as a website, postal mail, or email. Submit comments once by whichever method works best for you; duplicate comments are disregarded.

FOR FURTHER INFORMATION CONTACT

This lists who you can ask if you have general questions about the system of records.

> **Tips**
>
> This could be either the name and email address of a specific person or a generic title and "info" email address at the agency. You may not receive a reply before comments are due. If it is after the comment deadline, the contact information may not be current.

Finding a Current Contact

If the contact information is out of date, or you are otherwise not receiving a response, here are some other strategies to try to locate the appropriate contact:

- Each agency is required to have a privacy page, which should have contact information: www.[agency].gov/privacy. But not all agencies have the required page.
- Every agency is required to have a "Senior Agency Official for Privacy," sometimes called "Chief Privacy Officers." Some agencies house this function in the Office of the Chief Information Officer (OCIO). The agency's staff directory or the agency's OCIO website can help you locate these people.
- The people that run the program that the system of records supports may be able to help. The agency's program website may have a contact email or phone number.

SUPPLEMENTARY INFORMATION

> **This section is merely explanatory.** It is usually the bulk of the preamble.

Background information about the proposed SORN, including a description of any changes being made to the system of records and the purpose(s) of the changes. This is the agency's description of what it intends to do with the system of records and why it believes the activities described to be appropriate, allowable, or necessary. There are no rigid requirements for the scope or detail of this information.

> **Tips**
>
> Read this section last. The other sections are binding; this section is not. Because it isn't binding, reading it first can bias your review. Check the binding sections first to see what the agency is actually doing, then read this to see if their explanation matches.

SIGNATURE

This is the name, title, and signature of the head of the agency responsible for the notice.

> **Tips**
>
> You are unlikely to comment substantively on this section. Official guidance instructs agencies to place this at the end of the preamble, but agencies occasionally and incorrectly place it at the end of the whole notice.

The System of Records Notice (SORN)

This part of the FRN is legally binding. The agency must follow exactly what is written here.

SYSTEM NAME AND NUMBER

This is a unique name for the system of records that clearly identifies the purpose or character of the system of records AND a unique identifying number. Frequently this corresponds to the name and number used in security control functions, like the Information Technology (IT) system inventories required by OMB Circular A-130.

> **Tip**
>
> You are unlikely to comment substantively on this section.

SECURITY CLASSIFICATION

This states whether any information in the records is classified.[4] If the records are classified, the agency can claim an exemption such that they don't have to show individuals the contents of the records the agency has about them. To claim that exemption, the agency must issue a proposed and final rule under the Administrative Procedure Act.

> **Tips**
>
> Realistically, you can check to make sure the exemption is being properly claimed. Beyond that to comment effectively, you would need to independently know whether the records contain classified information and the general character of those records. If they are classified, the review requires specialized skill beyond the scope of this document.

> **Question for Consideration:**
>
> ❑ Is there a (k)(1) EXEMPTION proposed for the system of records to protect the classified records from access?

For More Information on...

Security classifications and controlled unclassified information, see Executive Orders 13526 *Classification, De-Classification, and Public Availability of National Security Information* and 13556 *Controlled Unclassified Information*

4 Note that the underlying frameworks for classification attach to the information itself, regardless of which entity possesses the data. Privacy protections work differently; they depend on who is holding the data.

SYSTEM LOCATION

This is the physical location of the system of records (city and state). If they are in more than one place, an appendix may be provided with the complete mailing address for every location housing a portion of the records. If a contractor is operating or maintaining the system of records, the contractor's name and location should be provided.

> **Tips**
>
> You are unlikely to comment substantively on this section. Physical location for electronic records may have little meaning today.

SYSTEM MANAGER(S)

This is the title, business address, and contact information of the agency official responsible for the system of records.

> **Tip**
>
> You are unlikely to comment substantively on this section.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM (This section is optional unless new or updated)

> This is a critical section to review.

This lists the authorities that authorize the collection and maintenance of records. Authorities include statutes (and associated regulations, if needed) or Executive Orders.

> **Tips**
>
> - Best practice is for the agency to provide both the title and the citation for each authority.
> - This section identifies the legal boundaries of what data an agency can collect and what it can do with it. For example, a law might require, permit, or prohibit certain actions. Or a law might put limits on data collection, use, or disclosure.
> - If you see a long list of all statutes that authorize agency activities, you should be suspicious. Ideally, there should be a short list of statutes that specifically authorize the program and the records.

Questions for Consideration:

- ❑ Does the cited authority adequately cover the activities described in the **PURPOSE**?
- ❑ Are all the relevant authorities cited? For example, if the **SUPPLEMENTARY INFORMATION** describes certain authorities as the basis for the agency's action, are these authorities also reflected here?
- ❑ Is the list of statutes specific and limited?

PURPOSE(S) OF THE SYSTEM (This section is optional unless new or updated)

> This is a critical section to review.

This should discuss the programmatic purpose that the system of records supports, that is, why the data was collected in the first place and how the information is used to carry out the program that collects or creates the records.

This section should discuss all purposes that support the original program collecting the records. This section should not discuss:

- **ROUTINE USES** (disclosures outside of the agency)
- *Need to Know* disclosures (within the agency for an authorized purpose)
- The **RECORD SOURCE CATEGORIES** (where the data comes from)

In effect, the **PURPOSE** defines the scope of the system. All other sections of the SORN and many of the statutory exceptions are evaluated against the **PURPOSE** described here.

> **Tips**
>
> Agencies often describe disclosures of records even if they are not a part of the original program purpose. This is not correct. If those descriptions stay, they broaden the **PURPOSE** inappropriately. (Note that there is no requirement to notify individuals or the public of internal disclosures that may happen after the original collection.)

Questions for Consideration:

- ❑ Has the agency adequately described why it is collecting the records and how it uses the records to carry out the relevant program?
- ❑ Is the purpose too broad? (*Are multiple unrelated purposes pigeon-holed into the notice? Is it so vague as to be unclear what type of records would be appropriately collected*? *If so, the **PURPOSE** may grant the agency undue latitude to disclose records, within or outside of the agency.)*
- ❑ Is the agency's **PURPOSE** clearly justified by the stated **AUTHORITY**?
- ❑ Are the purposes appropriate given the described?
- ❑ Is the agency describing disclosures within the agency? These shouldn't be in the SORN but may give you useful information about the agency's intentions.
- ❑ Is the agency discussing how the records will be used for a different program outside of the agency? Such discussion should happen under **ROUTINE USES**.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM (This section is optional unless new or updated)

> This is a critical SORN section to review. This dictates who has Privacy Act rights with respect to the records.

This is also known as the "covered populations" section and describes the specific individuals (living citizens or legal permanent residents, not businesses) whose records are maintained. It may discuss the agency's policy on granting administrative Privacy Act rights to non-U.S. Persons in a *mixed system*. This description should be specific and avoid using broad descriptions.

Questions for Consideration:

- ❑ Is the population described with enough specificity to understand who is included?
- ❑ Are the categories of individuals those that you would expect given the **PURPOSE** of the collection and the agency publishing the notice?
- ❑ Are any populations that you would expect to see missing from the notice?

Finding Out What is Actually Collected From the Public

If the information is collected from the public, you can cross reference this description with materials used to collect it. To do so, you will want to look at the Information Collection Instruments (such as forms) associated with the system of records on reginfo.gov. To find the right listing, "Search" under the "Information Collection Review" tab for the agency, sub agency, or program. You can also search by the specific form name, form number, or OMB control number, if you know them (they might be listed in the SORN). It may be helpful to limit your results under "ICRs That" by selecting "Include a form that requires a Privacy Act Statement [5 U.S.C. § 552a(e)(3)]." However, that filter isn't always accurately populated.

In the appropriate listing, **review the *"IC List"* or *"Information Collection Instruments."*** To see the individual forms, select an individual information collection (IC) title; the forms and instructions are linked from this "View Information Collection (IC)" page. You will know you have the right forms if this page includes a cross reference back to the name and most recent *Federal Register* listing for the SORN you're reviewing. However, the SORN cross reference information isn't always accurately populated, so you might have the right form even if that cross reference is absent or points to a different SORN.

For More Information on...

Mixed systems, Refer to APDU's Issue Brief, *Managing "Mixed Systems" of Records Under the Privacy Act of 1974*, available at https://apdu.org/apdu-in-action/data-privacy-resources

CATEGORIES OF RECORDS IN THE SYSTEM (This section is optional unless new or updated)

This is a critical SORN section to review.

This describes the actual records collected and maintained in the system of records. While agencies usually describe classes or types of data, OMB guidance says they should include specific data elements (like Date of Birth, or Name) *"if practicable and useful for public notice."* An accurate and informative description is especially important because this SORN might be the only place this context may be available to the public.

The agency should only collect and maintain information needed for the **PURPOSE** of the program; the agency may not collect information solely for a secondary use.

Tips

- It is important to understand that a system of records may not have a 1:1 relationship with how information is collected or stored, for example a specific form or IT system. Under the Paperwork Reduction Act (PRA), most information collected from the public must be approved by OMB and posted publicly in an Information Collection Request (ICR).

  A system of records may include:

  - Records with information from multiple ICRs (such as surveys)
  - Records with only some of the information in an ICR (such as forms)
  - Records not subject to the PRA (such as federal personnel records)
  - Records in one, multiple, or zero IT systems

- Spotting mismatches: There are many ways that there could be a mismatch between the program **PURPOSE**, the **CATEGORIES OF RECORDS** the agency is collecting, and the **ROUTINE USES** of those records. Here are two hypothetical examples that illustrate how you can compare this section to the **PURPOSE**, **ROUTINE USES**, or the ICR to assess 1) how appropriate these records are and 2) how transparent the SORN is:
  - Invisible records: Imagine that a **ROUTINE USE** only makes sense if the agency were collecting geographic data, but there is no geographic data described in this section. You can check the ICR to see if geographic data is being collected. If it is, it should be listed here. If it isn't being collected the **ROUTINE USE** may not be appropriate.
  - Unnecessary records: Suppose the program **PURPOSE** doesn't need income information, but income is described here or in the ICR. In this case, either the agency should not be collecting income, or the **PURPOSE** doesn't fully describe the authorized program. It is not enough for a **ROUTINE USE** to need the information.

Questions for Consideration:

- ❑ Are the records described with enough specificity for the public to understand what is being collected and maintained? Sample probing questions:
  - Does the agency provide a list of data elements (such as street number, street, or ZIP code) or categories of data that make sense (such as home address)?
  - If a form is referenced, is the form described and the form number provided?
- ❑ Are any categories missing from the notice that you would naturally expect to see?
- ❑ Does each category of records included in the SORN:
  - support at least one of the agency's stated **PURPOSES,** AND
  - not solely support an unrelated use or future disclosure of the data

You can try to cross reference this information with the actual materials used to collect the data by using the Information Collection tips mentioned above.

RECORD SOURCE CATEGORIES (This section is optional unless new or updated)

This is a general description of where the agency obtains the records (such as directly from the individual, from another agency, from a state or local grantee, purchased from a private sector company). Also describes the method of collection (such as a form, interview, scan).

An agency should collect data directly from the individual "to the greatest extent practicable." If the data isn't collected directly from the individual, the individual will not receive a direct notice about the existence of the records. Note that the SORN may be exempt from collecting directly from the individual (such as law enforcement records).

Questions for Consideration:

- ❑ Are the sources what you would expect to see and appropriate given the **PURPOSE**?
- ❑ Does the record come from another federal program? If so,
  - Is this use consistent with the purposes of that program?
  - If from another federal agency, does the other agency have a **ROUTINE USE** for this disclosure? You would have to find and review the other agency's SORN to ascertain this.

❑ Is the agency being "lazy" and trying to avoid collecting information directly?

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES (This section is optional unless new or updated)

This is a critical SORN section to review. This is one of the most misunderstood sections of a SORN.

A **ROUTINE USE** is a disclosure of records outside of the agency without individual consent. The agency must establish each routine use in this section of the SORN and update the SORN with any substantial changes. The routine use should not duplicate or water down an existing statutory disclosure and it should not restate an existing programmatic purpose.

The **ROUTINE USE** must be *compatible* with the **PURPOSE** for which the record is collected. Three major types of routine uses may qualify as *compatible*:

1. The program **PURPOSE** is ***directly related*** to the need for disclosure; that is, the routine use advances the purpose for which the program collects the data.
   - *Example:* agencies share employee data with contractors to process payroll.
2. The routine use is **necessary and proper** to the administration of the program and especially to upholding the integrity of the program.
   - *Example:* to allow the National Archives and Records Administration (NARA) to inspect records under its statutory responsibilities.
3. **Collateral** uses that may be unrelated to the purpose for which the information was collected, but Congress enacted a law requiring the disclosure.
   - *Example:* IRS shares tax return information with HHS to determine eligibility for participation in a state children's health insurance program under title XXI of the Social Security Act.

Routine uses must state to whom and for what purpose the record may be disclosed. They should be narrowly tailored. For example, "to other Federal Agencies as required" is NOT sufficiently specific. It should specify the portions of records to be disclosed, if not the full record.

For example, this common routine use clearly specifies:

1. To whom the records are going.

Records from this system of records may be disclosed to the **National Archives and Records Administration or to the General Services Administration** for **records management inspections** conducted **under 44 U.S.C. 2904 and 2906**.

2. Why they are being disclosed, which is both necessary and proper (to make sure the program is keeping its records appropriately) and is required by another law
3. And that purpose is narrowly defined (it must fall under these parts of law).

Tips

Common reasons (that is, "purposes") for a routine use include:

- **Litigation** – for example, to send records to the Department of Justice in its role to represent the agency, or to file records in a court proceeding
- **Constituent Services** – to Members of Congress or their staff so that they can assist with a constituent's request, such as the status of a benefits application
- **Taking legal action** – such as when the agency discovers fraud and refers it to the appropriate agency for investigation and related law enforcement activities
- **Investigative interviews** – to provide enough information so a potential witness knows what the inquiry is about
- **Records management** – to allow NARA to inspect records
- **Contractors** – disclosing to companies who have been hired to help run a program

Specific and careful language is still needed to mitigate privacy concerns.

If the **ROUTINE USE** only applies to a subset of the records, then the scope of the system of records might not be well defined. This should be in the **PURPOSE**.

Transfers of records have two sides: the sender (this SORN) and the receiver. If this disclosure is to an agency, the receiving SORN should (but doesn't always) reflect receipt of these records in its **RECORD SOURCE CATEGORIES**. You can review the receiving SORN to understand the potential risks and benefits of disclosing the records.

Privacy Act protections only apply to agencies;[5] if this disclosure is to an entity that is not an agency (such as Congress, purely advisory offices in the White House, or a state agency) these protections no longer apply to the disclosed records in the hands of the recipient.

Questions for Consideration:

- ❑ For each disclosure, did the agency include both
  - to whom record will be disclosed AND
  - for what purpose?
- ❑ Is each disclosure *compatible* with the **PURPOSE** of record collection? (directly related, necessary and proper, or collateral)
- ❑ Is each disclosure narrowly tailored to the specific purpose of the routine use?
- ❑ Are the records of sufficient quality for the intended purpose of the disclosure?
- ❑ Does it only allow the data elements relevant to the disclosure's purpose to be disclosed? (Reference the **CATEGORIES OF RECORDS**)
- ❑ Is the disclosure appropriate given how the records are collected (**RECORD SOURCE CATEGORIES**)?

5 A Privacy Act agency is a federal executive branch cabinet-level agency (or the highest level of a non-cabinet agency), excluding parts of the Executive Office of the President that are primarily advisory in nature. See 5 U.S.C. § 552a(a)(1) or APDU's *Primer on the Privacy Act of 1974* for a full definition and discussion, available at https://apdu.org/apdu-in-action/data-privacy-resources/.

- ❑ Does the agency avoid duplicating or watering down statutory disclosures?
- ❑ If the disclosure is a transfer to another agency, is the receiving agency also updating the SORN for the receiving system of records?
- ❑ Is the agency establishing the routine use because it is too "lazy" to seek consent from individuals?

For More Information on...

- Routine uses, see APDU's Issue Brief, *The "Routine Use" Exception of the Privacy Act of 1974* https://apdu.org/apdu-in-action/data-privacy-resources/Whats-a-Routine-Use/.
- Statutory disclosures (i.e., exceptions) see APDU's *Primer on the Privacy Act of 1974* https://apdu.org/apdu-in-action/Data-Privacy-Resources/Privacy-Act-1974/.
- Both, see Office of Privacy and Civil Liberties, Department of Justice, *Overview of the Privacy Act of 1974* (2020 Edition), *available at* www.justice.gov/opcl/overview-privacy-act-1974-2020-edition.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS (This section is optional unless new or updated)

This describes the media used to store records. Examples: "automated, maintained in computer files;" "manual, maintained in paper files;" or "hybrid, maintained in paper files and electronic media."

Tip

You are unlikely to comment substantively on this section.

For more information, see OMB Circular No. A-130

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS (This section is optional unless new or updated)

This describes how the records qualify as a *system of records* by retrieving records using a personal identifier. If personal identifiers are not used to retrieve records, then it isn't a system of records, and the Privacy Act doesn't apply.

This section should name specific data elements that are used to retrieve a particular individual's record. It should not list anything that is not a personal identifier.

Also, it is possible for multiple systems of records to be linked, for example within the same IT system. If searching for a record in this system of records automatically pulls up records in a different SORN, per OMB guidance the agency should explain this linkage here.

Questions for Consideration:

- ❑ Does the agency include the personal identifiers used to retrieve records, without superfluous information about other data elements?
- ❑ If there is a connection to another SORN, what implications does this notice have for the other records? (for example, how should it affect access procedures?)

For more information, see OMB Circular No. A-130

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS

(This section is optional unless new or updated)

This describes how long the agency keeps the records and how the records are destroyed, if they are ever disposed of. It should reference and describe the NARA records schedule and the agency's implementation procedures. The schedule is king. If the NARA schedule changes, the SORN must be updated to match.

The NARA schedule describes 1) whether the records will be archived permanently and 2) what will happen to any copies of the records the agency has (they may be either retained or destroyed after a certain time or event).

Tips

- It's common for this to be a pro forma entry because NARA has not yet approved the records management schedule; records are treated as permanent until approved.
- "Transfer to NARA" does not mean "agency destroys its copy." The agency should describe what is happening to the agency copy even if it sends a copy to NARA.

Questions for Consideration:

- ❑ Does the SORN indicate whether, when, and how records are retained? destroyed?
- ❑ Does the SORN cite a NARA Records Schedule or state that one is being prepared?

NARA Retention Schedules

If the SORN references an existing NARA schedule, it may either be:

- a General Record Schedule (GRS) available at https://www.archives.gov/records-mgmt/grs.html or
- an agency-specific schedule, which should be available at https://www.archives.gov/records-mgmt/rcs or on the agency intranet.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS (This section is optional unless new or updated)

This describes the security protocols in place to protect the records, including the administrative, technical, and physical safeguards. This shouldn't be so detailed that it would compromise the security of the records, but it should say more than "only people with a need to know have access." It should say how access is limited to those people, such as screening practices, like background checks, and with locked doors and cabinets, passwords, badges, or log sheets.

Tip

If **LOCATION** discusses cloud-based data, this should describe how that is managed.

For more information, see OMB Circular No. A-130

RECORD ACCESS PROCEDURES (This section is optional unless new or updated)

This is the procedure for an individual to access, review, or obtain a copy of their record(s).

CONTESTING RECORD PROCEDURES (This section is optional unless new or updated)

This is the procedure for an individual to contest or request an amendment to their record(s).

NOTIFICATION PROCEDURES (This section is optional unless new or updated)

This is the procedure for an individual to check whether records exist about themselves.

EXEMPTIONS PROMULGATED FOR THE SYSTEM (This section is optional unless new or updated)

This is a comprehensive discussion of all Privacy Act exemptions the agency is claiming. If an exemption is claimed, there should be an accompanying rulemaking that appears in the *Federal Register* on the same day. You should review the SORN and rule together.

> **Tip**
>
> **Exemptions remove Privacy Act rights**; they should be reviewed with the greatest care. However, a detailed review of exemptions is beyond the scope of this guide

Privacy Act Exemptions

- An overview of potential exemptions is available in APDU's Primer on The Privacy Act of 1974
- For additional detail, see Office of Privacy and Civil Liberties, Department of Justice, Overview of the Privacy Act of 1974 (2020 Edition), available at www.justice.gov/opcl/overview-privacy-act-1974-2020-edition.

HISTORY

This lists relevant history related to the SORN. If the SORN is a revision, this should include citation(s) to the last full *Federal Register* notice that includes all of the sections that are required to be in a SORN, as well as any subsequent notices of revision.

> **Question for Consideration:**
>
> ❑ Does the SORN include complete historical information and citations?

Pragmatic Cross-cutting Reviews

As you review, pay attention to two pragmatic and holistic questions: Did the agency follow the rules (procedure)? and Is the SORN practical?

Did the agency follow the correct rules? (administrative procedure)

If an agency doesn't follow the correct procedure, they may need to stop operating under the SORN until they fix the errors, such as by issuing a corrected SORN.

> **Questions for Consideration:**
>
> ❑ Did the agency adhere to the appropriate timelines?
>
> - Check the **DATES**, there should be at least 30 calendar days between SORN publication and
> - the deadline for the public to comment on the routine uses.
> - the date the routine uses actually go into effect.

- **EXEMPTIONS**. If the agency claims an exemption, did they publish a "Notice of Proposed Rulemaking" or an "Interim Final Rule" in the *Federal Register* on the same day as the SORN?

❑ Is contact and process information included?

- These sections should include the name or title of an appropriate individual and an email or website: **ADDRESSES**, **FOR FURTHER INFORMATION CONTACT**, and **SYSTEM MANAGER(S)**.
- The **RECORD ACCESS**, **CONTESTING RECORD**, and **NOTIFICATION** should be consistent with the agency's published procedures and clearly state:
  - Who you should contact and how to submit a request.
  - What information you need to provide so the agency can find your records.
  - What proof of identity you need to show.

❑ Does the notice follow the correct *Federal Register* format and OMB Guidance? Example questions for relatively common errors:

- Are all relevant and required SORN sections included? For example, if the system of records is new, are all SORN sections included?
- Is the notice signed by the highest agency official? (**SIGNATURES**)

❑ Does the notice indicate that the agency has transmitted the notice for review to:
  - the Office of Management and Budget?
  - both houses of Congress?

  Notices are only required if the agency establishes or makes a significant change to a system of records. The agency is not required to include this indication, but it is best practice (usually in the **SUPPLEMENTARY INFORMATION** or **HISTORY**).

Is the SORN Practical and Appropriate?

A SORN fails its purpose if it is impossible to understand or implement.

Questions for Consideration:

❑ Is the SORN written in clear, plain language?

❑ Does the **SUPPLEMENTARY INFORMATION** match the actual rules in the SORN?

❑ Are **RECORD ACCESS**, **CONTESTING RECORD**, and **NOTIFICATION** procedures clear and reasonable?

❑ Would the **CATEGORIES OF RECORDS** and **ROUTINE USES** achieve the **PURPOSE** described?

Useful Guidance Resources

1. OMB Circular A-108: *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*. https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A108/omb_circular_a-108.pdf
2. Implementing Regulations: *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28,948 (July 9, 1975), available at https://www.govinfo.gov/content/pkg/FR-1975-07-09/pdf/FR-1975-07-09.pdf
3. The Privacy Act of 1974, codified at 5 USC §552a.
4. OMB Circular A-130: *Managing Information as a Strategic Resource* (July 2016) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
5. Paperwork Reduction Act: Comprehensive guidance is available https://pra.digital.gov/

APPENDIX A:
SORN REVIEW CHECKLIST

The checklist prioritizes the sections to review and summarizes the key questions.

If you only have half an hour…

PURPOSE

- ❑ Has the agency adequately described why it is collecting the records and how it uses the records to carry out the relevant program?
- ❑ Is the **PURPOSE** too broad?
- ❑ Is the agency's **PURPOSE** clearly justified by the stated **AUTHORITY**?
- ❑ Are the purposes appropriate given the **CATEGORIES OF INDIVIDUALS** described?
- ❑ Is the agency inappropriately describing disclosures within the agency?
- ❑ Is the agency discussing how the records will be used for a different program outside of the agency? (Such discussion should happen under **ROUTINE USES**.)

CATEGORIES OF INDIVIDUALS

- ❑ Is the population described with enough specificity to understand who is included?
- ❑ Are the categories of individuals those that you would expect given the **PURPOSE** of the collection and the agency publishing the notice?
- ❑ Are any populations that you would expect to see missing from the notice?

CATEGORIES OF RECORDS

- ❑ Are the records described with enough specificity for the public to understand what is being collected and maintained?
- ❑ Are any categories missing from the notice that you would naturally expect to see?
- ❑ Does each category of records included in the SORN support at least one of the agency's stated **PURPOSES**, AND not solely support an unrelated use or future disclosure of the data?

ROUTINE USES

- ❑ For each disclosure, did the agency include both to whom the record will be disclosed AND for what purpose?
- ❑ Is each disclosure *compatible* with the **PURPOSE** of record collection?
- ❑ Is each disclosure narrowly tailored to the specific purpose of the routine use?
- ❑ Are the records of sufficient quality for the intended purpose of the disclosure?
- ❑ Does the routine use only allow the data elements relevant to the disclosure's purpose to be disclosed? (Reference the **CATEGORIES OF RECORDS**)
- ❑ Is the disclosure appropriate given how the records are collected? (Reference the **RECORD SOURCE CATEGORIES**)
- ❑ Does the agency avoid duplicating or watering down statutory disclosures?
- ❑ If the disclosure is a transfer to another agency, is the receiving agency also updating its receiving SORN?
- ❑ Is the agency establishing the routine use because it is too "lazy" to seek consent from individuals?

If you have more time…

HAS THE AGENCY FOLLOWED THE CORRECT ADMINISTRATIVE PROCEDURE?

- ❑ Did the agency adhere to the appropriate timelines?
- ❑ Is contact and process information included?
- ❑ Does the notice follow the correct *Federal Register* format and OMB Guidance?
- ❑ Does the notice indicate that the agency has transmitted the notice for review to OMB and both houses of Congress?

IS THE SORN PRACTICAL AND APPROPRIATE?

- ❑ Is the SORN written in a clear, plain English?
- ❑ Does the **SUPPLEMENTARY INFORMATION** match the rules in the SORN?
- ❑ Are **RECORD ACCESS**, **CONTESTING RECORD**, and **NOTIFICATION** procedures clear and reasonable?
- ❑ Would the **CATEGORIES OF RECORDS** and **ROUTINE USES** achieve the **PURPOSE**?

AUTHORITY FOR MAINTENANCE OF THE SYSTEM

- ❑ Does the cited authority adequately cover the activities described in the **PURPOSE**?
- ❑ Are all the relevant authorities cited?
- ❑ Is the list of statutes specific and limited?

SECURITY CLASSIFICATION

- ❑ Is a (k)(1) **EXEMPTION** proposed for the system of records to protect from access?

RECORD SOURCE CATEGORIES

- ❑ Are the sources what you would expect to see and appropriate given the **PURPOSE**?
- ❑ Does the record come from another federal program, and is this use consistent with the purposes of that program?
- ❑ If from another federal agency, does that agency's **SOURCE** system of records have a **ROUTINE USE** for this disclosure?
- ❑ Is the agency being "lazy" and trying to avoid collecting information directly?

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS

- ❑ Does the agency include the personal identifiers used to retrieve records, without superfluous information about other data elements?
- ❑ If there is a connection to another SORN, what implications does this notice have for the other records?

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS

- ❑ Does the SORN indicate whether, when, and how records are retained? destroyed?
- ❑ Does the SORN cite a NARA Records Schedule or state that one is being prepared?

HISTORY

- ❑ Does the SORN include complete historical information and citations?