

Introducing searchable PII Inventory

Demo and Q+A with the Federal Privacy Council's
AIC

March 23, 2020

18F

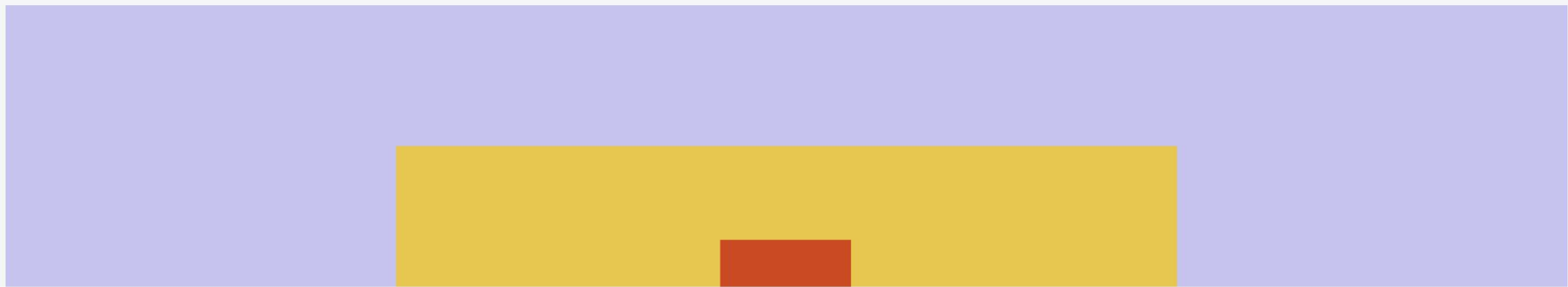
in partnership with 10x

We're here to:

- **introduce a searchable PII inventory that we've been developing with the GSA privacy office**
- **invite all of you to help us shape this work**

18F partners with agencies to improve the user experience of government services by helping them build and buy technology.





10x is an incremental investment fund inside the United States federal government. We fund internal projects that can scale across the federal government or significantly improve how our government builds technology for the public good.

**How did this PII
inventory project
begin?**

We started with a question:

How might we make it easier for privacy offices to manage the PII within their networks?

After holding interviews with government employees who work in privacy offices, manage IT systems, and work at the program level, we learned about many complex challenges around handling PII - many that would be outside of scope for us (like setting policies).

But we found one way to apply our engineering and design skills: to help speed up manual processes that slow privacy offices down.

Problem:

Privacy offices are burdened with managing compliance paperwork, and this reduces their bandwidth for proactive efforts to protect the public's privacy.

We developed a searchable PII inventory to give privacy offices some time back. Here are some activities that this inventory would speed up:

- finding information about PII from PIAs and SORNs
- understanding the landscape of PII that you manage
- producing an inventory as per OMB Circular A-130 requirements
- improving PII collection practices by system owners
- minimize PII collection to only that which is legally authorized/mission-essential

Demo

Use case 1

Joe, who works in a federal privacy office, understands that OMB Circular A-130 directs her office to take steps to reduce unnecessary use of social security numbers as a personal identifier. But taking on this task can be laborious.



"I have to look through all of our PIAs to find out which systems collect SSNs. That will take some time."

PII Inventory

Questions? Contact gsa.privacyact@gsa.gov

Old Prototypes Table Layout

FILTERS

QUICK FILTERS

☒ SSN ☐ email

CUSTOM FILTERS

TYPE

☐ SORN ☒ PIA

System

SORN ID

PII

ACTIVE FILTERS: Showing 16 of 85

PII: SSN

Ancillary Financial Application (AFA) system

Type: PIA

SORN ID: GSA/PPFM-11

PII:

- bank account information
- contract numbers
- DUNS Number
- e-mail address
- history of payments.
- home address

- home phone
- invoice number
- **SSN**
- TIN
- Name

[Source](#)

Beta.SAM.gov

Type: PIA

SORN ID:

By allowing Joe to perform a search of PIAs for IT systems that collect SSNs, she can see immediately the GSA PIAs collect SSNs.

With this, Joe can focus on reaching out to system points of contact and helping them identify alternative identifiers to use.

Use case 2

Now that Joe has the list of systems that process SSNs, she wants to see her agency's SORNs that list SSN as a "categories of records in the system". That way, she can crosswalk them against the PIAs with SSNs. If there are any discrepancies, she'll be able to find them and take next steps to make corrections.



"I want to make sure the our Federal Register records are accurate."

PII Inventory

Questions? Contact gsa.privacyact@gsa.gov

Old Prototypes Table Layout

FILTERS

QUICK FILTERS

☒ SSN ☐ email

CUSTOM FILTERS

TYPE

☒ SORN ☐ PIA

System

SORN ID

PII

Search

ACTIVE FILTERS:

Showing 2 of 85

PII: SSN

GSA Credential and Identity Management System (GCIMS).

Type: SORN

SORN ID: GSA/CIO-1

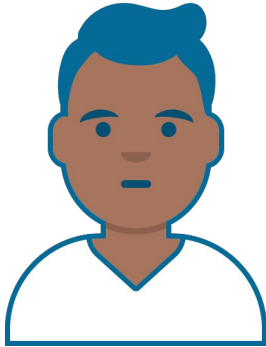
Categories of Record:

- Citizenship
- Company name
- contract base number (Contractors only)
- Contract company (also referred as vendor) (Contractors only)
- Contract end date (Contractors only)
- Contract option years (yes or no) (Contractors only)
- Contract start date (Contractors only)
- Date of birth
- Date of entry (Non-US citizens only)
- Date of issuance of security clearance
- Investigation results and date
- Less than 3-year US resident (yes or no) (Non-US citizens only)
- Level of security clearance
- Name of prime if company is subcontractor (Contractors only)
- Names of previous companies on GSA contracts (Contractors only)
- Occupation
- Organization/office of assignment
- Physical and logical access
- Place of birth
- Port of entry city and state (Non-US citizens only)
- Region

By filtering her SSN search by SORNs, she can see the GSA SORNs that list SSN as a category of record.

Use case 3 (if this were public facing . . .)

Kris, a member of the public who has worked as a government contractor, wants to see which IT systems have his home address. He knows that he can submit a Privacy Act request but doesn't know which systems to ask about.



"I just moved and want to make sure that the records are up to date."

FILTERS
QUICK FILTERS
☐ SSN ☐ email
CUSTOM FILTERS
TYPE
☐ SORN ☒ PIA
System

SORN ID

PII

Search

ACTIVE FILTERS: Showing 13 of 26 results for "home address"

Ancillary Financial Application (AFA) system
Type: PIA
SORN ID: GSA/PPFM-11
PII:

- bank account information
- contract numbers
- DUNS Number
- e-mail address
- history of payments.
- home address
- home phone
- invoice number
- SSN
- TIN
- Name

[Source](#)

CWTSatoTravel
Type: PIA
SORN ID: GSA/GOVT-4
PII:

- air
- alternative address
- alternative telephone number
- hotel
- hotel reservations
- individual charges and balances

By conducting a search, Kris can locate the systems that are relevant for him. He can then include them in his Privacy Act request, making the request easier for GSA's privacy team to process.

What's next

Ensuring that this first version of a PII inventory is sustainable for GSA to manage without us.

To do this, we've built using technology that the GSA already relies on. All the data sits in a Google spreadsheet that they can access and edit. The web application is static and the code is open source so that any new dev team can access it.

Making this PII Inventory available for other government teams to use.

We'll be uploading this PII inventory to NIST's Privacy Framework Resource Repository to increase its findability. Our work is open source so that other agency developers can take our code (at no cost) and use it to build a similar tool for their own privacy team. We plan to develop documentation to make it easier for others to use our work.

Exploring whether there are other agencies that would want to work with us.

We're still looking for opportunities to help other agencies build PII inventories of their own. Please reach out if you'd like to discuss this with us: privacy_devops@gsa.gov

Building out new features.

We'd like to expand the types of information that this PII inventory includes. Some areas that we are considering adding are: authority, information sharing agreements, FISMA level, retention policies, a way to compare content between PIAs and SORNs that cover the same IT system.

We'd love to hear your perspective on what would be most valuable. You can let us know by filling out [this survey](#).

Thanks!

Contact 18F@gsa.gov

Follow [@18F](https://twitter.com/18F)

Work Together github.com/18F