



# Design research

## *Privacy Impact Assessment*

July 28<sup>th</sup>, 2017

**POINT of CONTACT**

**Richard Speidel**

Chief Privacy Officer, GSA IT

1800 F Street, NW

Washington, DC 20006

[richard.speidel@gsa.gov](mailto:richard.speidel@gsa.gov)

# Table of contents

## **SECTION 1.0 PURPOSE OF COLLECTION**

- 1.1 Why is the information being collected?
- 1.2 What legal authority and/or agreements allow the information to be collected?
- 1.3 Is the information searchable by a personal identifier – like a name or Social Security number? If so, what Privacy Act System of Records Notice(s) apply/applies to the information being collected?
- 1.4 Is there a records retention schedule that has been approved by the National Archives and Records Administration (NARA) for the information system(s)? Explain how long and for what reason the information is retained.
- 1.5 Are there any forms or surveys that are associated with the collection of the information that would be covered by the Paperwork Reduction Act (PRA)?
- 1.6 Are there any privacy risks for this system that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

## **SECTION 2.0 OPENNESS AND TRANSPARENCY**

- 2.1 Will individuals be given notice prior to the collection of personal information about them? If not, please explain.
- 2.2 Will individuals be given notice prior to their information being shared? If not, please explain.
- 2.3 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

## **SECTION 3.0 DATA MINIMIZATION**

- 3.1 Whose information is included in the system?
- 3.2 What PII will the system include?
- 3.3 Why is the collection and use of the PII necessary to the project or system?
- 3.4 Will the system aggregate previously unavailable data about the individual or create new data about the individual? If so, how will this data be maintained and used?
- 3.5 What controls exist to protect the consolidated data and prevent unauthorized access?
- 3.6 Will the system monitor the public?
- 3.7 Will the system monitor employees or contractors?
- 3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?
- 3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

## **SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION**

- 4.1 Is the information in the project limited to only the information that is needed to carry out the purpose of the collection?

- 4.2 Will 18F share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?
- 4.3 Is the information collected directly from the individual or is it taken from another source?
- 4.4 Will the project interact with other systems, whether within GSA or outside of GSA? If so, how?

### **SECTION 5.0 DATA QUALITY AND INTEGRITY**

- 5.1 How will the information collected be verified for accuracy and completeness?
- 5.2 Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

### **SECTION 6.0 SECURITY**

- 6.1 Who will have access to the data in the project? What is the authorization process for access to the project?
- 6.2 Has 18F completed a system security plan for the information system(s) supporting the project?
- 6.3 How will the system be secured?

### **SECTION 7.0 INDIVIDUAL PARTICIPATION**

- 7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.
- 7.2 What procedures will allow individuals to access their information? If so, how?
- 7.3 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

### **SECTION 8.0 AWARENESS AND TRAINING**

- 8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.
- 8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

### **SECTION 9.0 ACCOUNTABILITY AND AUDITING**

- 9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?
- 9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

## Document purpose

GSA uses design research to better understand the experiential aspects (such as usability) of the digital products and services it builds, and to better understand the contexts in which such digital products and services are used. Incident to its design research practice, GSA may collect personally identifiable information (PII) about people. PII is any information<sup>1</sup> that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

This document contains important details about GSA's collection and use of information, both standardized and nonstandardized<sup>2</sup>, in its conduct of design research. GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, shares, and destroys information in a way that protects privacy. GSA PIAs are broken out into sections reflecting the goals of its [privacy program](#). These sections also align to the Fair Information Practice Principles (FIPPs), a set of precepts codified in the Privacy Act of 1974.<sup>3</sup>

## Project

Design research

## Project/system includes information about

Federal employees, contractors, and members of the public

## Project/system includes

---

<sup>1</sup>OMB Memorandum *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (OMB M-07-16) defines PII: "information which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

<sup>2</sup> HHS's *Frequently Asked Questions About PRA / Information Collection* explains that data collections are standardized "whenever each respondent or group of respondents is asked to provide the same level of information on the same subject." OMB Memorandum *Flexibilities under the Paperwork Reduction Act for Compliance with Information Collection Requirements* clarifies: "[OIRA] does not generally consider facts or opinions obtained through direct observation by an employee or agent of the sponsoring agency or through nonstandardized oral communications in connection with such direct observations to be information under the PRA."

<sup>3</sup> Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

Design research collects data across two broad categories: administrative data and study data.

Administrative data is data collected and used during the recruiting and administration of a design research study. Administrative data includes:

- **Respondent data** is data such as voluntarily submitted name, contact information (for example, telephone number or email address), reason for visiting the digital product or service, and goals for use. When necessary, this may also include demographic information such as age range, education level, language, profession, occupation, etc.
- **Respondent metadata** is data indirectly collected as a result of the media (for example, the web form) through which a respondent indicates their interest in participating in design research. It may include data such as timestamp, operating system, and user-agent (browser).
- **Administration trace data** is data used to facilitate the administration of design research. For example, GSA may record having contacted a respondent for an interview or having received a participant's signature on an informed consent form.

Study data is data collected during a design research study. This may include, with consent, photo, video, or audio recording and transcription of individuals. Specifically, study data includes:

- **Contextual data** is data describing context of use. This includes, but is not limited to, descriptions of workplaces, workaday interactions, and existing business processes; perceptions, use, and valuations of products, services, and regulations; relevant literacies; and the success of existing outreach and educational efforts.
- **Direct feedback** is data collected directly from participants about products and services, such as responses, anecdotes, and assessments.

## Overview

General Services Administration's Technology Transformation Service (TTS) aims to improve the way government builds, buys, and maintains digital products and services. Accordingly, TTS leverages approaches to service delivery originally pioneered in government by the Presidential Innovation Fellows (PIFs), the Consumer Financial Protection Bureau (CFPB), and the US Digital Service<sup>4</sup>. One such approach is design research.

The spirit of design research at GSA is not new. For example, GSA's Office of Customer Experience has practiced similar methods since its inception. TTS has simply collaborated with stakeholders across GSA to more formally establish this approach and assess potential privacy risks in a transparent way.

[Executive Order 13571](#), *Streamlining Service Delivery and Improving Customer Service*, Section 2 (B) states that "agencies shall establish mechanisms to solicit customer feedback on government services and, using such feedback, shall regularly make improvements to government services." GSA's design research practice is directly aligned with Executive Order 13571.

Design research broadens perspectives and tests assumptions by actively and systematically engaging with information ecosystems. Design research includes both qualitative and quantitative research methods such as meeting with stakeholders to learn about a project, investigating and comparing tools and systems, and interacting with members of the public. It also includes the use of questionnaires, surveys, and analytics.

GSA refers to this activity as *design* research because of its relationship to higher-order decisionmaking. Specifically, GSA uses design research to: (1) help better understand the experiential aspects (such as usability) of products and services, (2) better understand the contexts in which digital products and services are used, (3) inform design hypotheses, and (4) validate design decisions.

---

<sup>4</sup> For a summary of their best practices, see the Digital Services Playbook at <https://playbook.cio.gov/>

Contextual integrity is essential to design research. GSA stands to derive the most realistic and actionable insights from studies that do not interfere with its customers' normal behaviors nor distort their opinions. For that reason, GSA chooses the recruiting methods, research methods, as well as the settings for its design research on a per-study basis. GSA also considers factors such as cost, anticipated response rates, and desired data formats. GSA's [Method Cards](#) describe its most frequently practiced design research methods. GSA chooses the setting for its studies across three broad categories, including: in-person (for example, interviews or workshops); remote, synchronous (for example, telephone or video conversations); and remote, asynchronous (for example, via discussion forums, email, social media, and web analytics).

Design research is performed as authorized by law. In addition, GSA uses social science research practices such as informed consent forms and operational security protections.

Design research may lead to the creation of design research artifacts, such as research reports<sup>5</sup>, personas, journey maps, and mental models. GSA maintains descriptions of and templates for such artifacts in its [Design Wiki](#). GSA assesses the sensitivity of its artifacts and applies appropriate risk-based mitigations<sup>6</sup> before sharing them. For example, GSA either de-identifies its artifacts or seeks the consent of individuals who would be identified by its artifacts.

GSA may contract or partner with third parties in its conduct of design research. As appropriate, GSA may identify individuals to act as contracting officer's representatives (CORs), lead studies, train third parties with whom it collaborates, and monitor third party performance. GSA proactively informs anyone who participates in design research of its inherent privacy risks and the steps GSA takes to mitigate them. GSA may also utilize contracts to ensure that third parties meet privacy and security requirements.

---

<sup>5</sup> See, for example, [this report](#) concerning customer perceptions of the 18F website.

<sup>6</sup> GSA recognizes that there may be sensitive information other than PII in its design research artifacts, and will protect that information as necessary in accordance with law and regulation. For example, in accordance with FAR 3.104-4, if GSA encounters any contractor bid information, proposal information, or source selection information during the course of its design research activities, that information will not be shared with unauthorized persons.

Participation in design research is voluntary. Individuals who respond expressing a desire to participate (respondents) and demonstrate that they meet the study's selection criteria may be selected for participation ("participants"). A person's responses (or lack thereof) in the course of a design research study can in no way affect that person's eligibility for or access to any government benefit, service, or position.

When necessary, GSA may use recruitment protocols to explain the voluntariness, outline the purpose, and indicate the desired participants in its design research. GSA recruitment protocols are written in plain language to be as accessible as possible. Individuals may be recruited through a variety of means, including but not limited to: introductions via the agencies with whom GSA works, snowball sampling<sup>7</sup>, installing popups on existing products or services ("live recruiting"), code repositories, social media, fliers, mailing lists, cold calling, or using a recruiting agency.

Most design research methods only require a single interaction between GSA and participants. Some methods however, such as a diary study, may require multiple interactions. In cases where multiple interactions are necessary, participants are provided advanced notice that their participation in the study requires multiple interactions or collections of information over an established period of time. Likewise, participants are informed of their opportunities to consent to future interactions or ongoing information collection. GSA may follow up with a participant for the purposes of concluding a single design research study.

Design research can present risks related to confidentiality, misuse of information, and opportunities for notice and informed consent. Risks related to **confidentiality** are present any time information could be used in an unauthorized manner. This is particularly relevant to design recruitment and administration, since individuals who respond to GSA recruiting protocols are effectively indicating some degree of association with the study's area of inquiry – imagine,

---

<sup>7</sup> Snowball sampling is a technique in which existing study subjects are asked to identify potential research subjects from among their acquaintances.

for example, a study to help improve access to information about infectious diseases. An individual's mere interest or participation could be confidential.

Breaches in confidentiality can potentially make individuals more vulnerable to harm or embarrassment. To reduce this risk, GSA trains its employees to properly handle data collected and used in the conduct of design research; stores administrative data separate from study data; applies appropriate minimization rules<sup>8</sup> to study data before subjecting it to shared analysis; designs its recruitment materials and protocols so as not to collect sensitive information about those it seeks to recruit; and uses security controls to protect information used in the conduct of design research.

Risk related to **misuse of information** may involve the collection and use of information without the participant's consent. Misuse of information can also include reuses of information for secondary types of design research that are incompatible with the purposes of the initial collection. To reduce this risk, GSA: minimizes access to data collected throughout a design research study to those with a need-to-know basis; stores administrative data separate from study data; and applies appropriate minimization rules to study data before subjecting it to shared analysis.

Finally there is a risk that participants may not fully understand the ways in which their information may be collected and used in GSA's design research. GSA helps mitigate this risk through **notice and consent opportunities**. GSA trains its staff to inform individuals that (1) their participation is voluntary and (2) the specific ways in which their information may be collected and used. GSA further explains its use of information through appropriate vehicles such as Privacy Impact Assessments, System of Record Notices, Privacy Act Notices, and informed consent forms.

GSA relies on multiple systems to support its design research. Information used for design research purposes is maintained within GSA authorized computing

---

<sup>8</sup> GSA uses minimization rules to prevent the unauthorized retention and use of personally identifiable information in its conduct of design research. For example, GSA redacts all information that is directly identifying from its written notes, including driver's license numbers and Social Security numbers. When appropriate, GSA blurs sensitive information captured in its photos and videos.

environments, including but not limited to [GSA's Enterprise Organization of Google Applications](#). This system is implemented across various vendors as well as GSA applications, all of which are part of the Enterprise Cloud Services (ECS) system. This system is commonly referred to as GSA/CIO-3. Information not contained within the GSA/CIO-3 system is contained in authorized contractor environments, where all system details are documented and reported to GSA on a recurring basis.

## SECTION 1.0 PURPOSE OF COLLECTION

*GSA states the purpose and legal authority for collecting PII.*

### 1.1 Why is the information being collected?

GSA collects this information to help meet the mandate of Executive Order 13571, Section 2 (B), which requires agencies to establish mechanisms to solicit customer feedback on Government services and using such feedback regularly to make service improvements.

GSA collects **administrative data**, including voluntarily submitted respondent data and metadata, for recruiting and administration purposes. These purposes include, for example, filtering respondents, scheduling participation, and conducting follow-up.

GSA collects **study data** to: (1) better understand the experiential aspects (such as usability) of products and services, (2) better understand the contexts in which digital products and services are used, (3) inform design hypotheses, and (4) evaluate design decisions.

### 1.2 What legal authority and/or agreements allow the information to be collected?

GSA's design research is authorized by Executive Order 13571, Section 2 (B).

### 1.3 Is the information searchable by a personal identifier – like a name or Social Security number? If so, what Privacy Act System of Records Notice(s) apply/applies to the information being collected?

No. Administrative data is indexed and retrieved via *project* identifier rather than a personal identifier (for example, “project one, sprint one<sup>9</sup>, respondent one; project one, sprint one, respondent two; etc.”), and study data is subject to appropriate minimization rules for PII de-identification. GSA's minimization rules for design

---

<sup>9</sup>A “sprint” is part of an [agile, iterative software development](#). It is a tightly scoped unit of work, usually no more than two weeks in duration. As part of its overall de-identification strategy, GSA aggregates administrative data by project and sprint rather than by any reference to personal identifiers.

research normally preclude searching by Social Security number or other identifier.

**1.4 Is there a records retention schedule that has been approved by the National Archives and Records Administration (NARA) for the information system(s)? Explain how long and for what reason the information is retained.**

GSA maintains and disposes of design research computer and paper records in accordance with [NARA's General Records Schedule \(GRS\) 3.1-011, "General Technology Management Records - System Development Records](#). GSA destroys these records at maximum either (1) five years after a given system is superseded by a new iteration, terminated, or defunded; or (2) when the records are no longer needed for agency/IT administrative purposes.

**1.5 Are there any forms or surveys that are associated with the collection of the information that would be covered by the Paperwork Reduction Act (PRA)?**

Yes. In conducting design research, GSA may seek OMB approval under the PRA through one of its generic clearances, including: [OMB Control Number 3090-0297](#), "Generic Clearance for the Collection of Qualitative Feedback on Agency Service Delivery (GSA)."

When GSA conducts design research on in collaboration with other agencies, it may collaborate with PRA desk officers at those agencies. Any additional PRA packages which are cleared may be reviewed at [Reginfo.gov](#).

**1.6. Are there any privacy risks for this system that relate to the purpose of the collection? If so, how will GSA mitigate these risks?**

Yes. The purpose of design research depends on the research question(s) or area(s) of inquiry driving any given study. Such purposes present privacy risks related to inappropriate collection, use, and disclosure of PII.

GSA mitigates these risks in different ways. First, as a practical matter, GSA limits its studies to areas where it stands to learn the most about the systems it might affect in the shortest time possible. This inherently reduces the risk that it might inappropriately collect PII.

GSA further mitigates risk through appropriate training, access controls, and minimization rules. To the extent that GSA receives more PII than necessary in the course of design research, it minimizes retention to reduce the possibility that PII may be misused subsequent to collection. For example, whenever GSA records photos or videos taken during a workshop, it employs appropriate minimization rules to remove or redact sensitive PII *before* incorporating that material into any sort of collective analysis. GSA only retains design research information for as long as it is necessary to support its mission in accordance with approved records retention schedules.

GSA may conduct design research in collaboration with, or on behalf of, other government agencies. When it does so, GSA collaborates with such agencies to meet any applicable privacy requirements. If necessary, GSA contracts and interagency agreements will define the conditions under which GSA is expected to share design research data with the other government agency.

Finally, GSA outlines appropriate uses and access controls for PII whenever it enters into agreements with third parties; for example, through data-sharing agreements or contracts. Outside of its use of third-party recruiting firms (to collect administrative data), GSA generally requires third parties to remove any PII prior to submitting data to GSA.

## **SECTION 2.0 OPENNESS AND TRANSPARENCY**

*GSA is open and transparent. GSA tells individuals about the PII it collects and how it protects, uses, and shares PII. GSA provides a straightforward way for individuals to learn about what is happening to their PII.*

### **2.1 Will individuals be given notice prior to the collection of personal information about them? If not, please explain.**

Yes. GSA uses both recruitment protocols and informed consent forms to explain the voluntariness, outline the purpose, and indicate the desired participants of its design research. These materials and protocols are written in plain language to be as accessible as possible. Individuals may be recruited through a variety of means, such as: introductions via the agencies with whom GSA works, installing popups on existing products or services (“live recruiting”), code repositories, social media, fliers, mailing lists, cold calling, or using a recruiting agency.

GSA may provide design research Privacy Act Notices in a variety of ways: in person, over the phone, via email, in hardcopy, and online. GSA has published a design research Privacy Act Notice on [its website](#). In some cases, respondents are provided an opportunity to request a hard copy of the notice in addition to having it provided in another medium.

GSA does not maintain a pool of volunteers from which to recruit. In the event that GSA contracts with a third party to recruit for or conduct design research on its behalf, GSA ensures that the third party uses appropriate recruitment protocols and informed consent forms. As appropriate, GSA’s contracts may include audit provisions authorizing GSA to audit contractors to ensure they provide individuals with copies of [its Design Research Privacy Act Notice](#) and comply with other contract requirements.

### **2.2 Will individuals be given notice prior to their information being shared? If not, please explain.**

Yes. Individuals are notified of how GSA may use the information collected from design research-recruiting activities on [its website](#). However, design research studies typically do not rely on direct identifying PII for analysis. To the extent that GSA seeks to publish or share information that directly identifies individuals, it will first seek the individual's consent.

**2.3 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?**

Yes, there is a risk that participants may not fully understand that GSA is conducting the design research, especially when third parties are involved. To mitigate this risk, GSA identifies itself, as appropriate, in materials associated with its design research. This includes but is not limited to recruitment protocols, informed consent forms, and information collection instruments.

## SECTION 3.0 DATA MINIMIZATION

*GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.*

### 3.1 Whose information is included in the system?

The desired participants in GSA's design research vary depending on the systems considered, the research questions addressed, and the methods of data collection employed. Respondents often include federal employees, contractors, and members of the public, though groups of particular interest are those who develop training materials for, make use of, or are impacted by digital products and services. In the past, for example, 18F has collected information from respondents who were applying for permits to use public land, and reporters who were making use of data provided by the Federal Election Commission (FEC).

### 3.2 What PII will the system include?

Administrative data may contain PII. Administrative data is data collected and used during the recruiting and administration of a design research study.

Administrative data includes:

- **Respondent data** is data such as voluntarily submitted name, contact information (for example, telephone number or email address), reason for visiting the digital product or service, profession, and goals for use. When necessary, this may also include demographic information such as age range, education level, language, occupation, etc.
- **Respondent metadata** is metadata collected at time of response, such as timestamp, operating system, and user-agent ("browser").
- **Administration trace data** is data used to facilitate the administration of design research. For example, GSA agents may record having contacted a respondent for an interview or having received a participant's signature on an informed consent form.

Study data, defined above, generally does not include PII before it is subjected to analysis.

### **3.3 Why is the collection and use of the PII necessary to the project or system?**

Direct identifying PII may be collected for the recruiting and administration of a design research study. This includes, for example, activities such as: scheduling participation, and conducting follow-up research as appropriate. Direct identifying PII collected for research administration is kept separate from study data.

Design research does not typically rely on direct identifying PII for analysis. Study data is used to generate insight into patterns of awareness, experiences, and decision-making across study participants. When GSA collects study data that contains direct identifying PII, those direct identifying PII are generally removed in accordance with appropriate minimization rules.

In certain cases, before the application of minimization rules, GSA may contact participants for permission to use or share their PII in a broader context. For example, subject matter experts may wish to receive attribution for feedback they have provided as part of their professional duties. In such cases, this PII is used to enrich the findings of a design research study and would only be used if specifically authorized by the subject matter expert.

### **3.4 Will the system aggregate previously unavailable data about the individual or create new data about the individual? If so, how will this data be maintained and used?**

No. GSA's design research will neither aggregate previously unavailable data about an individual, nor will it create new data about an individual. GSA applies appropriate minimization rules to its study data so as to prohibit the compilation of data on specific individuals.

### **3.5 What controls exist to protect the consolidated data and prevent unauthorized access?**

GSA protects personal information relevant to design research as described in Section 6, Security, below.

### **3.6 Will the system monitor the public?**

GSA may use information that is passively collected through programs such as its Digital Analytics Program in the course of Design Research, however these programs do not collect PII and hence pose no privacy risk.

GSA informs and obtains the voluntary consent of any individual it seeks to observe or monitor in the course a study.

### **3.7 Will the system monitor employees or contractors?**

Use of the GSA network and storage devices that maintain the design research information is audited in accordance with [GSA IT Security Procedural Guide: Audit and Accountability \(AU\) CIO-IT Security-01-08](#).

### **3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?**

Design research does not produce reports on individuals; rather, design research may lead to the creation of artifacts describing the information ecosystems in question. These artifacts may include (but are not limited to) research reports, personas, journey maps, and mental models.

Design research artifacts are based on aggregate information which has itself already been subjected to appropriate minimization rules. Research artifacts are occasionally illustrated by photographs or quotations. In certain cases, before application of its minimization rules, GSA may contact participants for permission to use or share their PII in a broader context. For example, GSA may

wish to use a photo collected during a study in a blog post. In such cases, GSA obtains the consent of participants prior to disclosure.

**3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?**

Participation in design research is voluntary, and GSA informs and solicits the voluntary consent of its study participants. Accordingly, individual respondents may choose what information they wish to provide. Subsequent to collection, GSA reduces the risk of having collected unnecessary PII through the application of appropriate minimization rules.

## **SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION**

*GSA publishes a notice about how it plans to use and share the PII that it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.*

### **4.1 Is the information in the project limited to only the information that is needed to carry out the purpose of the collection?**

Yes. Direct identifying PII is necessary to conduct recruiting for, and to facilitate the administration of, design research. GSA stores and secures this information separately from the information collected during the studies themselves.

### **4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?**

Although design research is primarily conducted to aid GSA's service delivery, GSA may administer design research in collaboration with, or on behalf of, other government agencies. When it does so, GSA works to meet applicable privacy requirements both at GSA and at the agencies with whom it collaborates. GSA uses contracts to define the conditions under which it is expected to share design research data.

Design research may lead to the creation of design research artifacts, such as research reports, personas, journey maps, and mental models. GSA may make versions of such artifacts available after assessing the sensitivity of each artifact and applying risk-based mitigation strategies, for example de-identifying the data or seeking consent from the individuals involved.

### **4.3 Is the information collected directly from the individual or is it taken from another source?**

The majority of data upon which design research relies is collected directly from individuals. Two types of data, however, rely on indirect collection: respondent

metadata and contextual data. Respondent metadata is indirectly collected as a result of the media (for example, the web form) through which a respondent indicates their interest in participating in design research. It may include data such as timestamp, operating system, and user-agent (“browser”). Contextual data often contains information captured by GSA in the course of a design research study. For example, GSA may, with its participant’s permission, take pictures of the participant’s place of work following an interview.

#### **4.4 Will the project interact with other systems, whether within or outside of GSA? If so, how?**

Most systems, such as contractor systems supporting design research, are not directly integrated with any other GSA system. All data transfers are manual; that is, they are executed by qualified personnel between contractor systems, vendor websites, and GSA internal systems via encrypted tunnels. These transfers can also take place via encrypted email. Some data that supports the design research will come from GSA internal systems, and the outside interactions of those systems will be documented in those systems’ Security Plans (SSPs).

#### **4.5 Are there any privacy risks for this project that relate to use limitation? If so, how will GSA mitigate these risks?**

Design research does not generally rely on direct identifying PII for analysis. To the extent that information collected contains direct identifying PII, there may be risk of unauthorized use. To mitigate this risk, GSA restricts the collection of and access to direct identifying PII. When partnering with a third party, for example, GSA typically restricts the third party from furnishing direct identifying PII to GSA through contract provisions and data-sharing agreements; GSA requires that study data be stored separately from administrative data.

To mitigate the risk of re-identification and monitoring of individuals, GSA limits personnel access to direct identifying PII to those with a role-based need to know using technical access controls, and provides appropriate privacy and security training so that personnel know how to handle and protect data. As appropriate, GSA may identify individuals to act as contracting officer’s representatives

(CORs), lead studies, train third parties with whom it collaborates, and monitor third party performance. GSA proactively informs anyone who participates in design research of its inherent privacy risks and the steps GSA takes to mitigate them.

GSA does not attempt to re-identify information that has been stripped of direct identifying PII, and may be contractually prohibited from doing so. GSA further reduces the risk of unauthorized disclosures by reviewing documents related to design research in light of legal requirements, including the Privacy Act, so that information is not inappropriately disclosed.

## **SECTION 5.0 DATA QUALITY AND INTEGRITY**

*GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.*

### **5.1 How will the information collected be verified for accuracy and completeness?**

GSA primarily collects information directly from participants, which ensures that the information is as accurate as possible. Further, GSA uses best practices from industry (specifically from design-led companies and consultancies) to plan its studies and manage their associated data. In addition, when GSA partners with a third party, it outlines appropriate standards for data accuracy and completeness in its contracts.

### **5.2 Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will GSA mitigate these risks?**

Contextual integrity is essential to design research; GSA stands to derive the most realistic and actionable insights from studies that do not interfere with its customers' normal behaviors nor distort their opinions. Accordingly, GSA chooses its recruiting methods, research methods, as well as the setting for its design research on a per-study basis.

Each design research method may pose a unique privacy risk. For example, moderated usability studies may pose privacy risks due to the extent to which researchers are able to read information that is ambiently present on a user's screen. As appropriate, GSA will proactively inform participants of the extent to which its choice of study method/setting poses privacy risks. GSA also employs appropriate minimization rules to proactively reduce the information it captures.

Finally, to reduce the risk related to data quality and integrity, GSA uses best practices of social science research design and data management techniques to reduce the impact of errors or bias in design research.

## **SECTION 6.0 SECURITY**

*GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

### **6.1 Who will have access to the data in the project? What is the authorization process for access to the project?**

GSA grants access to information collected via design research only to personnel who have a need to know. As appropriate, GSA may empower specific personnel to lead studies, train collaborators, monitor performance, and inform participants of potential privacy risks and the steps GSA takes to mitigate them.

When GSA collaborates with other researchers to conduct design research, it uses both legal and non-disclosure agreements to restrict access to data, as appropriate.

Design research may lead to the creation of design research artifacts, such as research reports, personas, journey maps, and mental models. GSA assesses the sensitivity of its research artifacts, and applies risk-based mitigations before sharing them. For example, GSA either de-identifies its artifacts or seeks the consent of individuals that would be identified by its artifacts.

### **6.2 Has GSA completed a system security plan for the information system(s) supporting the project?**

Yes, GSA has completed system security plans (SSPs) for the systems that support and maintain the information used for design research. GSA categorizes all of its systems using Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems (FIPS 199). Typically, design research is conducted on systems rated “moderate impact.” Based on this categorization, GSA implements security controls from NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations” to secure its systems and data.

### **6.3 How will the system be secured?**

GSA assesses information and systems for compliance risk, reputational risk, strategic risk, situational/circumstantial risk, and operational risk. In order to mitigate these risks to an acceptable level, GSA implements extensive security controls for information collected or maintained on its behalf, and conducts third-party assessments of vendors and services it procures.

GSA implements the following controls for internally maintained systems: GSA policies and procedures governing privacy and information security; background checks on all personnel with access to the system; initial and follow-on privacy and security awareness training for each individual with access to the system; physical perimeter security safeguards; Security Operations Center (SOC) to monitor antivirus and intrusion detection software; risk and controls assessments and mitigation; technical access controls, such as role-based access management and firewalls; and appropriate disaster mitigation strategies, breach notification processes and plans, and secure channels for submitting information.

GSA implements controls relevant to third party vendors and services according to risks identified the following types of third party reviews: Third Party Security Assessment and Authorization (SA&A) Package; Statements on Standards for Attestation Engagements (SSAE) Review; Risk Assessments by Independent Organization; or a complete Risk Assessment by GSA.

### **6.4 Are there mechanisms in place to identify security breaches? If so, what are they?**

GSA has [procedures](#) in place for handling security incidents. GSA monitors use of its systems and is responsible for reporting any potential incidents directly to the relevant Information Systems Security Officer. This Officer coordinates the escalation, reporting and response procedures on behalf of GSA.

### **6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?**

There is always some potential risk of unauthorized use or disclosure of PII. GSA mitigates the risk of privacy incidents by providing privacy and security training to GSA personnel on the appropriate use of information and implementing breach notification processes and plans.

In addition, access is limited on a need to know basis, with logical controls limiting access to data. GSA also automates protections against overly open access controls. For example, GSA's CloudLock tool searches all GSA documents stored in Google Drive for certain keyword terms and removes the domain-wide sharing on these flagged documents until the information is reviewed. GSA agents can then review the flagged items to ensure no sensitive information has been accidentally placed in or inadvertently shared via these files.

## SECTION 7.0 INDIVIDUAL PARTICIPATION

*GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.*

**7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.**

**Unmoderated** design research studies typically require little-to-no interaction between GSA and study participants because data collected during unmoderated studies is often unidentifiable. For example, GSA may study unidentifiable usage metadata collected under its Digital Analytics Program. Individual participation in unmoderated design research studies may be obligatory (that is, not voluntary); per [FTC guidance from 2010](#), GSA informs individuals of passive data collections by way of its websites' respective privacy policies and terms of use.

**Moderated** design research studies, on the other hand, may require sufficient interaction between GSA and study participants. For example, GSA may ask individual participants to share their screen and explain their goals and current uses of an information system. Participation in moderated studies is always voluntary. When recruiting for a moderated study, GSA informs individuals via a recruitment protocol – for example, a website popup that says “Help us improve this website!” – containing [a Privacy Act Notice](#). Individuals may also receive an informed consent form in which they can acknowledge their free and informed choice to participate.

GSA's informed consent forms for design research are [based on a publicly available template](#); they include a [Privacy Act Notice](#). These consent forms may also include, as appropriate: a statement of the purposes of the research; the expected duration of the study; a description of the research methods employed; a description of any reasonably foreseeable risks or discomforts to the participant; a description of the benefits or results that can reasonably be expected from the research; a description of the extent, if any, to which

confidentiality of records identifying the subject is maintained; a point of contact to address any questions; necessary language for the government to accept gratuitous services, and a statement that participation is voluntary, refusal to participate involves no penalty, and the subject may discontinue participation at any time without penalty.

Once individuals choose to participate, they generally cannot restrict GSA's use of their information so long as GSA's use aligns with both: (1) those uses outlined in this PIA and (2) the previously agreed upon purposes of the study. Individuals who wish to opt out of design research *after* their information has been collected should direct their written correspondence to either their study point of contact or the point of contact shown at the top of this PIA.

## **7.2 What procedures will allow individuals to access or amend their information?**

Individuals may seek to access or amend **administrative data** about themselves in accordance with the Privacy Act and [the GSA's Privacy Act regulations](#), at 41 CFR Part 105-64 et seq.

**Study data** does not generally contain indexed information about or attributable to specific individuals. Individuals may amend their data only under certain circumstances. Specifically, if:

1. An individual has recently participated in a moderated study, and
2. That individual sends a written request to their study point of contact (or the point of contact shown at the top of this PIA) requesting access to their information, and
3. GSA has yet to apply its minimization rules to the study in question, and
4. GSA can reasonably identify and isolate that individual's data

then GSA can, at its discretion, provide that individual with access to their data and/or an opportunity to amend it (for example, to clarify a response, or to answer an outstanding question).

**7.3 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?**

Yes. Regardless of whether individuals choose to participate or not, GSA may create administrative-trace data acknowledging their choice. This information describes, at minimum, a potential relationship between an individual and GSA. GSA mitigates this risk through appropriate access controls to administrative data, by promoting transparency through this PIA, and through public comments to Information Collection Requests published in the Federal Register.

## **SECTION 8.0 AWARENESS AND TRAINING**

*GSA trains all personnel about the proper handling of PII.*

### **8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.**

GSA requires privacy and security training for all personnel and has policies in place that govern the [proper handling of PII](#).

### **8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?**

Yes. All GSA personnel engaged in design research are made aware of the potential risks inherent in design research through activities including but not limited to, town-hall events and presentations, Research Guild meetings, email reminders, and the publication of this PIA.

The conduct of design research involves risks that are similar to GSA's other interactions with its customers and the public. Therefore, design research poses minimal additional risk related to training. As appropriate, GSA may identify individuals to act as contracting officer's representatives (CORs), lead studies, train third parties with whom it collaborates, and monitor third party performance. GSA proactively informs anyone who participates in design research of its inherent privacy risks and the steps GSA takes to mitigate them.

## **SECTION 9.0 ACCOUNTABILITY AND AUDITING**

*GSA's privacy program is designed to make the agency accountable for complying with these principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.*

### **9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?**

GSA requires privacy and security training for all personnel, and has policies that govern the [proper handling of PII](#). GSA has also implemented security and privacy controls for its systems, including those that support design research, and has limited access to those personnel with a need to know. Further, OMB requires the GSA to document these privacy protections in submissions for Information Collection Requests processed under the Paperwork Reduction Act.

As appropriate, GSA may identify individuals to act as contracting officer's representatives (CORs), lead studies, train third parties with whom it collaborates, and monitor third party performance. GSA proactively informs anyone who participates in design research of its inherent privacy risks and the steps GSA takes to mitigate them.

All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately. As discussed above, GSA takes automated precautions against overly open access controls. GSA's CloudLock tool searches all GSA documents stored in Google Drive for certain keyword terms and removes the domain-wide sharing on these flagged documents until the information is reviewed. GSA agents can then review the flagged items to ensure no sensitive information has been accidentally placed in or inadvertently shared via these files.

### **9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?**

Yes. In keeping with NIST [800-53 rev 4, control number AR-4](#), GSA regularly assesses its programs to ensure effective implementation of privacy controls.

While some of these assessments can be automated, such as those carried out via GSA's CloudLock tool (mentioned above), others are carried out via GSA or third-party auditors.

Because they may receive privileged access to design research-related data, auditors can pose risks above and beyond those previously described. Specifically, auditors can pose risks to: (1) confidentiality, in the form of re-identification; and (2) misuse of information. Recall that one of the ways in which GSA mitigates the normal risk of re-identification is to separately index administrative data from study data. In order to properly ensure this separation, however, GSA auditors would need access to both. Furthermore, due to their privileged access, auditors would have the ability to subject disparate datasets to shared analysis.

To mitigate this risk, GSA clearly identifies personnel with the capacity to audit its design research program and provides them with appropriate role-based training. Auditors perform their duties in collaboration with GSA supervisors and/or GSA's Privacy Office.

## PIA Signatures

### Chief Privacy Officer

7/13/2017

X Jacquelyn Henry for Richar...

---

Richard Speidel  
Chief Privacy Officer, GSA IT  
Signed by: JACQULYN HENRY

### Chief Customer Experience Officer

7/17/17

X Anahita Reilly

---

Anahita Reilly  
Chief Customer Experience Officer

### Chief Information Security Officer

7/14/2017

X Kurt Garbars

---

Kurt Garbars  
Chief Information Security Officer, GSA IT  
Signed by: KURT GARBARS

## Participating Offices

### Office of Products and Platforms

X *Sarah Crane*

---

Sarah Crane  
Acting Assistant Commissioner, GSA Office of P...

18F

X *Russ Unger*

---

Russ Unger  
Experience Design Director, 18F

### Presidential Innovation Fellows

X **Nathan Olson**

Digitally signed by Nathan Olson  
DN: cn=Nathan Olson, o, ou,  
email=nathan.olson@gsa.gov,  
c=US  
Date: 2017.07.18 15:55:16  
-04'00'

---

Nathan Olson  
Acting Director, Presidential Innovation Fellows