Privacy Impact Assessment

Enterprise Mobile Devices

April 25, 2018

PART II. SYSTEM ASSESSMENT

A. Data in the System

Question	Explanation/Instructions
1. What is the specific purpose of the agency's use of the information and how does that use fit with the agency's broader mission?	EMD is a general support system supporting users at GSA. It is composed of mobile elements (smartphones, tablets and laptops) that process daily activities related to job performance.
1. Describe all information to be included in the system, including personal data.	Users may store PII data mobile devices that are supported by the EMD. Such information may include, but is not limited to, names, email addresses, phone numbers, mailing addresses, photos, credit card information for the purpose of in-app purchases and other financial information. *Smartphones and tablets can store any user input including name, address, phone number, credit card information etc. it is up to the user to be cautious with their Government Furnished Equipment (GFE) and use it as intended.*
1.a. What stage of the life cycle is the system currently in?	*Operation/Maintenance*
2.a. What are the sources of the information in the system?	The system contains commercial off the shelf (COTS) software for the purpose of performing job functions. The data that is processed is entered by the user.
2.b. What GSA files and databases are used?	Users can download files from GSA's instance of a Google drive. The files accessed will depend on the users job function and network permissions.
2.c. What Federal agencies are providing data for use in the system?	*GSA*
2.d. What State and local agencies are providing data for use in the system?	None
2.e. From what other third party sources will the data be collected?	None

2.f. What information will be collected from the individual whose record is in the system?	*None* *GSA does not require the user to input their data. It is left to user discretion on what personal information is stored.*
3.a. How will the data collected from sources other than Federal agency records or the individual be verified for accuracy?	All GSA Government Furnished Equipment (GFE) has encrypted hard drive. Only the user will have access to their device unless the user allows another access.
3.b. How will data be checked for completeness?	The PII is not required or recommended by GSA. The IT General Rules of Behavior "…GSA provides IT resources for official use, GSA does authorize users to utilize email and social media and access the Internet for personal use provided that users keep the use and access to a minimum and do not interfere with official system use or access." " Take measures to protect Personally Identifiable Information (PII) and sensitive data, …" CIO P 2100.1 "Ensuring Personally Identifiable Information (PII) and/or sensitive data stored on any workstations or mobile devices including, but not limited to, laptop computers, notebook computers … is encrypted with GSA provided encryption." "Ensuring GSA managed computers that collect and store PII must adhere to all PII requirements."
3.c. Is the data current? How do you know?	*It is inputted by the user for their personal use and is not regulated by GSA.*
4. Are the data elements described in detail and documented? If yes, what is the name of the document?	*The data is not collected by GSA nor is it recommended for storage on GFE.*

B. Access to the Data

Question	Explanation/Instructions
1. a. Who will have access to the data in the system?	*Only the user who inputs the data.*
1.b. Is any of the data subject to exclusion from disclosure under the Freedom of Information Act (FOIA)? If yes, explain the policy and rationale supporting this decision.	*No*
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	*It is the user who determines the access. GSA does not collect or recommend that PII be stored or processed on GFE. Users are required to sign the IT Security ROB and notified that any PII they store or process on GFE is their responsibility.*
3. Will users have access to all data in the system or will the users' access be restricted? Explain.	Users have access to their own work and any information they store or process on the GFE. The user controls the restrictions of access. GSA does not collect or recommend that PII be stored or processed on GFE.
4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?	Information on GFE is encrypted and only accessible from the user. Local Support can wipe a device but will not have access to the data stored or processed on GFE.
5.a. Do other systems share data or have access to data in this system? If yes, explain.	*No*
5.b. Who will be responsible for protecting the privacy rights of the clients and employees affected by the interface?	*No Interface*
6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	*None*
6.b. How will the data be used by the agency?	*No one other than the user will have access.*
6.c. Who is responsible for assuring proper use of the data?	*Only the user who inputs the data.*
6.d. How will the system ensure that agencies only get the information to which they are entitled?	*No one, other than the user, is entitled to the data.*

7. What is the life expectancy of the data?	GSA does not collect or recommend storage or processing of PII on GFE.
8. How will the data be disposed of when it is no longer needed?	When the life of the GFE is determined, Local Support will wipe the device in accordance with DoD requirements. Local Support will not have access to the data that has been stored or processed on the GFE.

C. Attributes of the Data

Question	Explanation/Instructions
1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	*No*
2.a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	*No*
2.b. Will the new data be placed in the individual's record (client or employee)?	*No*
2.c. Can the system make determinations about individuals that would not be possible without the new data?	*NO – the data is only accessible by the user who inputs the data.*
2.d. How will the new data be verified for relevance and accuracy?	*N/A – the data is provided by the user.*
3.a. If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.	*N/A*
3.b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	*N/A*
4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	*GFE is encrypted and is only accessible by the user whom the device is registered too. For accessibility to laptops, PIV is used; for smartphones and tablets a password or biometrics are used in access.*

5. What are the potential effects on the privacy rights of individuals of: a. Consolidation and linkage of files and systems; b. Derivation of data; c. Accelerated information processing and decisionmaking; and d. Use of new technologies. How are the effects to be mitigated?	The user can omit PII on their device. If the user chooses to store PII on GFE issued to them, they assume all liability for protecting that information. GSA uses due care when issuing GFE to the user with hard drive encryption enabled.

D. Maintenance of Administrative Controls

Question	Explanation/Instructions
1.a. Explain how the system and its use will ensure equitable treatment of individuals.	*N/A – GSA Does not collect PII on GFE.*
1.b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?	*N/A – GFE is mobile by it's nature.*
1.c. Explain any possibility of disparate treatment of individuals or groups.	N/A – data input is for personal use only.
2.a. What are the retention periods of data in this system?	*N/A – GSA does not collect PII on GFE.*
2.b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	*N/A – GSA does not maintain the data in GFE.*
2.c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	*N/A – GSA does not maintain the data in GFE.*
3.a. Is the system using technologies in ways that Federal agencies have not previously employed (e.g. Caller-ID)?	*No*
3.b. How does the use of this technology affect individuals' privacy?	*N/A*
4.a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	*The GFE user can locate the device using the Lookout application. However, no location info is shared with GSA, even if "location access" is enabled on the GFE.*
4.b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	*N/A*
4.c. What controls will be used to prevent unauthorized monitoring?	*Users are responsible for protecting the security of their GFE. Protection of GFE includes but not limited to signing the ROB, keeping PIV cards secure, keeping usernames and password combinations secure etc.*

5.a. Under which Privacy Act System of Records notice (SORN) does the system operate? Provide number and name.	*The EMD does not require coverage under a GSA system of records notice (SORN) because it does not retrieve information via a personal identifier.*
5.b. If the system is being modified, will the SOR require amendment or revision? Explain.	*N/A*