AmeriCorps
Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	**Name of the information system:**	OfficeSpace Software
1-2	**System Identifier (3 letter identifier):**	
1-3	**Unique Investment Identifier (Exhibit 53):**	
1-4	**Office or entity that owns the system:**	AmeriCorps Office of Facilities and Support Services (OFSS)
1-5	**Office or entity that operates the system:**	OfficeSpace Software Inc.
1-6	**State if the system is operational or provide the expected launch date:**	Operational
1-7	**System's security categorization:**	Low
1-8	**Date of most recent Security Assessment and Authorization (SA&A) or why one is not required:**	September 2023
1-9	**Approximate number of individuals with PII in the system:**	The approximate number of AmeriCorps employees with PII in the system are listed below. Currently, there are about 2,726 names in the system. The names are never deleted, the status can be either active or inactive, including place holder where a position hasn't been taken yet as no position is filled. When a position is filled, a name is entered for that place holder. Individuals with active records are approximately 1,034. In the administrator portion of the system there are about 851 users.

3 – SIGNATURES (ORIGINAL MAINTAINED BY CHIEF PRIVACY OFFICER)			
	Role	*Signature*	*Date*
3-1	Information System Owner:		
3-2	Office of General Counsel:		
3-3	Chief Privacy Officer:		
3-4	Chief Information Security Officer:		
3-5	Senior Agency Official for Privacy:		

4- PIA HISTORY	
4-1	**State whether this is the first PIA for the system or an update to a signed PIA.**
	First PIA
4-2	**If this is an update, describe any major system changes since the last PIA.** **If this is the first time a PIA is being completed, write Not Applicable.**
	Not Applicable
4-3 A	**State whether this is the annual review of PIA.**
	No
4-3 B	**Describe any changes to the system, data activity, policies, procedures, any interrelating component and process, vendor, 3rd parties, contracts and any required controls since last PIA.**
	First PIA
4-3 C	**Describe objects and results of audit or tests (continuous monitoring).**
	OfficeSpace undergoes third-party penetration testing on an annual basis and is subject to a System and Organization Controls (SOC) 2 report requirement every 12 months.
4-3 D	**Certify and state "Completion of Review" if no change occurs.**
	Interim Authorization to Operate (ATO) OfficeSpace system has been signed and approved by AmeriCorps.
4-4	**If the system is being retired, state whether a decommission plan is completed and attach a copy.**
	Not Applicable

5- SYSTEM PURPOSE	
5-1	**Describe Purpose of the System (or program, product, service)**
	OfficeSpace is a Computer Aided Facilities Management (CAFM) software of OfficeSpace Software Inc. that provides Space Allocation and Management Software Services. Officespace is web-based and is hosted in Google Cloud Platform (GCP). The Office of Facilities and Support Services (OFSS) uses the OfficeSpace Move and Scenario Manager, Reports, Visual Directory™ and Portal features to support agency's key operations, including space management such as seating assignments, moves, hybrid scenarios plans/ projects, help desk request and ticket management, and workspace booking that facilitate teleworkers to book hoteling stations. OfficeSpace enables AmeriCorps to optimize space usage, track space metrics, and measure and report the performance of OFSS in meeting the needs of AmeriCorps' workforce.

6- INVENTORY OF PII	
6-1	**Provide a list of all the PII included in the system.**
	The application utilizes AmeriCorps' official staff directory. The information includes federal employees' and contractors' names, business mailing addresses, business phone numbers, and business e-mail addresses.
	AmeriCorps staff might voluntarily submit information about their home address to the system when they make a shipping-related request, even though AmeriCorps provides instruction requesting that employees do not input personal shipping information into the system.

7- CATEGORIES OF INDIVIDUALS IN THE SYSTEM	
7-1	**Describe the categories of individuals whose PII is in the system and state approximately how many individuals are in each category.**
	The category of individuals whose PII is in the system includes AmeriCorps federal employees and contractors. The system currently maintains approximately 2,726 names; this number fluctuates on a regular basis. The total number of AmeriCorps staff with active records in the system are approximately 1,034. In the administrator portion of the system, there are about 851 users.

8- INFORMATION IN THE SYSTEM	
	For each category of individuals discussed above:

8-1 A	Describe the information (not just PII) collected about that category and how the information is used.
	OfficeSpace can utilize data such as the counts of AmeriCorps employees and contractors, floor plans, and basic employee information to generate reports related to help desk ticket performance metrics (completion time, time until first action, closure status, etc.), occupancy levels, and lease costs (not currently inputted in the software), etc. OfficeSpace only uses information provided by AmeriCorps, which includes the employee's or contractor's first and last name, department, supervisor information, phone number, business email address, business address, and job title (optional). Occasionally, AmeriCorps staff might choose to voluntarily submit their home address in order to receive mail from AmeriCorps; however, this practice is discouraged and noted within the system. When a new employee is onboarded, AmeriCorps pushes the new information to the OfficeSpace system. The information is then used for seating assignments, moves, hybrid scenarios plans and projects, help desk ticket management, and workspace booking. The application generates activity logs for users within AmeriCorps. The essential information that the audit logs collect includes user logins, system changes, file changes, and timing of events and activities. Audit logs also collect the browser type and the IP address of the devices that AmeriCorps staff use to access the system. The logs can monitor and track the activities of users. Officespace technical administration personnel have access to those audit logs. The OfficeSpace technical and customer support teams may have access to the data in AmeriCorps' OfficeSpace system for technical troubleshooting and investigation purposes.
8-1 B	State whether the system derives new data, or creates previously unavailable data, about an individual via aggregation of information or other means. Explain why, how it is related to the purpose of the system, how it is used and with whom it is shared.
	Not Applicable
8-1 C	If the system uses commercial or publicly available data, explain why, how it is related to the purpose of the system, and how it is used.
	Not Applicable
8-1 D	Describe any application of PII redaction, mask, anonymization or elimination.
	For system troubleshooting purpose, some data will be used for testing. Data de-identification is performed before the data is used for testing.
	Describe any design that is used to enhance privacy protection.

8-1 E	All data used by the system is encrypted in transit and at rest. OfficeSpace uses only data that is necessary for providing the service. The users of OfficeSpace can input notes and upload attachments when they are submitting help desk ticket requests. A warning is posted for each type of request (i.e., heating, ventilation, and air condition (HVAC), mail, security) to discourage users from inputting any PII that is not required. However, an employee or contractor might input a home address if they make a mail-related request, and they disregard the warning message.

9- COLLECTIONS OF PII INTO THE SYSTEM	

9-1	**Describe for each source of PII in the system:**
	   a. **The source.**
	   b. **What comes from that source.**
	   c. **How the PII enters the system.**

	The employee's or contractor's last name, first name, job title, department, supervisor, phone number, business email address, and business address that are entered into OfficeSpace are provided by AmeriCorps' official staff directory. The PII such as the name provided by AmeriCorps staff directly and voluntarily when they accept their job offer is used by this system for the purpose of maintaining the business operations of AmeriCorps. Information such as seat location, whether the employee or contractor is a remote worker, or the employee's or contractor's key fob number to enter the building are entered into the system by the OFSS staff member. An AmeriCorps employee or contractor might input a home address if they make mail-related requests, and they disregard the warning message of not to include such PII in their helpdesk request
9-2	**If any PII comes directly from the individual, describe the privacy controls in place. If all PII comes from a secondary source, write <u>Not Applicable</u>.**
	The system does not collect PII directly from AmeriCorps staff. AmeriCorps staff might voluntarily submit their home address information in their request to receive mail from OFSS despite the fact that they are directed not to provide this kind of information via office email. OFSS has a process in place that ensures this information will be deleted from OfficeSpace by a system administrator. All the information in the system is entered into the system via secured connections and encryption controls and is used only by authorized AmeriCorp personnel. All data stored in AmeriCorps' Office Space system is built on encrypted volumes and is protected and sealed from other Office Space customers.

9-3	If PII about an individual comes from a source other than the individual, describe:
	     a. Why the PII is collected from the secondary source.
	     b. Why the PII from the secondary source is sufficiently accurate.
	     c. If/how the individual is aware that the secondary source will provide their PII.
	 If all PII about an individual comes directly from the individual, write <u>Not Applicable</u>.

	Not Applicable
9-4	**If any collections into the system are subject to the Paperwork Reduction Act (PRA), identify the Office of Management and Budget (OMB) Control Number for the collection and effective date. If the system does not implicate the PRA, write <u>Not Applicable</u>.**
	Not Applicable
9-5	**If any collections into the system are subject to an agreement, describe those agreements. If no agreements are relevant, write <u>Not Applicable</u>.**
	Not Applicable

10- SYSTEM ACCESS	

10-1	**Separately describe each category of individuals who can access the system along with:**
	     a. **What PII they can access (all or what subset).**
	     b. **Why they need that level of access.**
	     c. **How they would request and receive that access.**
	     d. **How their access is reduced or eliminated when no longer necessary.**
	     e. **Identify policies and procedure outlining roles and responsibilities and auditing processes.**

	When AmeriCorps requests to book a room on OfficeSpace, AmeriCorps will send the information to the OfficeSpace administrator. The administrator who is an OfficeSpace Subject Matter Expert (SME) will retrieve the information from AmeriCorps, save it to AmeriCorps' official staff directory and send a notification to AmeriCorps to acknowledge receipt. The OfficeSpace administrator will only have access to the information that AmeriCorps sends to them to provide data processing services, and will make updates per AmeriCorps' notification and request. The OfficeSpace technical and customer support teams may have access to the data in AmeriCorps' OfficeSpace system for troubleshooting and investigation purposes.

The validity of the data is reviewed on a regular basis by OFSS. Some data, such as "Inactive People Assignments," is reviewed by the software. However, this data can be incorrect and is reviewed and compared manually to OfficeSpace's official staff directory to ensure accuracy. The "Preferences" contents are reviewed to ensure consistent department names are in place. Because data is manually entered into AmeriCorps' official staff directory, it often might include typos that are passed through to OfficeSpace. When found, these errors are corrected and the updated information is passed back to AmeriCorps personnel in charge of updating AmeriCorps' official staff directory. Very few changes are made to the PII on Office Space after it is entered into AmeriCorps' Office Space System.

At the end of the service contract, OfficeSpace administrator access is no longer needed and will be deleted. OfficeSpace will return the data to AmeriCorps by request or they will delete the data after 60 days of contract termination. OfficeSpace's data security policy, data classification standards, data retention standard, and SOC 2 report further specify their responsibilities for these data handling activities.

11- PII SHARING	

11-1	**Separately describe each entity that receives PII from the system and:**
	    a. **What PII is shared.**
	    b. **Why PII is shared** *(specify the purpose)*
	    c. **How the PII is shared (what means/medium).**
	    d. **The privacy controls to protect the PII while in transit.**
	    e. **The privacy controls to protect the PII once received.**
	    f. **PII sharing agreements (***describe if the agreement specifies the scope of the information sharing, parties of agreement and the duration of the agreement***)**
	    g. **Describe security and privacy clauses and audit clauses in the agreement or vendor (including third party vendors) contract.**
	
	If PII is not shared outside the system, write <u>Not Applicable</u>.

	The email addresses of AmeriCorps staff may be shared with Mailgun Technologies Inc., a 3rd party email provider that OfficeSpace retains for booking confirmation and notification purposes. Mailgun handles all of OFSS's OfficeSpace email notifications and reminders. Mailgun is included in Officespace's desk booking module. For example, when an AmeriCorps employee books a desk in OfficeSpace, the employee will receive a confirmation email with all of the details for the booking. These notifications and reminders are the only service that Mailgun handles. Mailgun only has access to

	users' business email addresses so as to be able to send out these notification emails.

12- PRIVACY ACT REQUIREMENTS

12-1	**If the system creates one or more systems of records under the Privacy Act of 1974:**
	    a. **Describe the retrieval that creates each system of records.**
	    b. **State which authorities authorize each system of records.**
	    c. **State which SORNs apply to each system of records.**
	If the system does not create a system of records, write <u>Not Applicable</u>.

	Not Applicable

13- SAFEGUARDS

13-1	**Describe the data processing environments and the technical, physical, and administrative safeguards (including vendors) that protect the PII in the system.**
	The OfficeSpace system is safeguarded through multiple layers of control to protect the information in the system. Administratively, all AmeriCorps employees are required to go through annual security and privacy training. AmeriCorps employees may be required to sign additional agreements before gaining access to OfficeSpace software information. In addition, the administrator users of OfficeSpace must sign an AmeriCorps Privileged User Rules of Behavior form and receive privacy and security training annually. AmeriCorps monitors and documents these required trainings to ensure adequate information security and privacy compliance posture is maintained. AmeriCorps' OfficeSpace application is a self-contained "software as a service" (SaaS) application hosted in GCP and managed by OfficeSpace. The Office Space data is stored on encrypted volumes. AmeriCorps' information is segregated from other information stored on Office Space and is protected by multiple layers of security including layered firewalls, intrusion prevention, and intrusion detection systems. Data can only be accessed after authentication and authorization has passed via OfficeSpace's privileged management system. All access is logged and alerted for irregularities. OfficeSpace's data security policy, data classification standards, data retention standards, and SOC 2 report further specify OfficeSpace's responsibilities for the data handling activities of AmeriCorps' OfficeSpace. Per the contract between AmeriCorps and the vendor, OfficeSpace Software, Inc., when the contract ends, OfficeSpace will return the data to AmeriCorps by request or they will delete the data after 60 days of contract termination. AmeriCorps has identified applicable record retention schedules for records in the system and is currently going through standarized record management processes to ensure the records in AmeriCorps'

		OfficeSpace will be appropriately handled and in accordance with record retention policies.
13-2		**Describe the technical, physical, and administrative measures that protect PII if the system is being retired.**
		Not Applicable.
13-3		**State if a system security plan and privacy plan is completed and the date of control verification.**
		OfficeSpace System Security and Privacy Plan was completed in December 2023.

14- DATA ACCURACY, ACCESS, AMENDMENT, AND CONTROL		
14-1		**Describe the steps taken to ensure PII is sufficiently accurate, relevant, current, and complete and the assurance procedure.**
		AmeriCorps provides the information from AmeriCorps official staff directory to be imported to OfficeSpace and makes updates when a new employee onboards. The information is current and relevant. Any inaccuracies must be corrected so that AmeriCorps can use OfficeSpace to book a room, make seating arrangements and successfully provide support service to AmeriCorps staff.
14-2		**Describe how an individual could view, correct, update, or ask to amend their PII.**
		All requests from AmeriCorps employees will be forwarded to AmeriCorps' system administrator for review and approval. Errors will be corrected once found or reported.
14-3		**Describe how an individual could control what PII about themselves is included in the system or how it is used. Also describe how those decisions could affect the individual.**
		All requests from AmeriCorps' employees will be forwarded back to AmeriCorps for review and approval.
14-4		**State if PII handling processes apply automation technology for decision making and describe the measures taken to eliminate risk to privacy interests.**
		Not Applicable

15- DATA RETENTION AND DESTRUCTION		
15-1		**Identify the National Archives and Records Administration (NARA) provided retention schedule for the system and provide a summary of that schedule.**

		The floor plans uploaded into OfficeSpace are not official records, rather copies. The plans, maintenance records, etc. are all saved and documented in SharePoint. Records retained that are related to Administrative Help Desk Records are covered by National Archives and Records Administration (NARA) General Records Scheduled GRS 5.4.010 (Disposition Authority DAA-GRS-2016-0011-0001) and 5.8.010 (Disposition Authority DAA-GRS-2017-0001- 0001). The disposition is temporary, and the records can be destroyed one year after the ticket/request is resolved, or when no longer needed for business use, whichever is appropriate.
15-1	**Identify the role and process to coordinate with the parties involved in record retention and disposition.**	
		The Information System Owner will coordinate the record retention activities with the agency records officer. OfficeSpace has internal data retention standards and policies documented in its Document Retention Standard.

16- SOCIAL SECURITY NUMBERS (SSNs)

16-1	**If the system collects truncated or full social security numbers (SSNs):**
	    a. **Explain why the SSNs are required.**
	    b. **Provide the legal authority for the usage of the SSNs.**
	    c. **Describe any plans to reduce the number of SSNs.**
	If the system does not collect any part of an SSN, write <u>Not Applicable</u>.	

		Not Applicable

17- WEBSITES

17-1	**If the system includes a website which is available to individuals apart from AmeriCorps personnel and contractors, discuss how it meets all AmeriCorps and Federal privacy requirements. If the system does not include a website, write <u>Not Applicable</u>.**	
		Not Applicable

18- OTHER PRIVACY RISKS

18-1	**Discuss any other system privacy risks or write <u>Not Applicable</u>.**	
		Not Applicable