AmeriCorps
Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	**Name of the information system:**	Webgrants
1-2	**System Identifier (3 letter identifier):**	DTW
1-3	**Unique Investment Identifier (Exhibit 53):**	
1-4	**Office or entity that owns the system:**	Office of Monitoring
1-5	**Office or entity that manages the system:**	Dulles Technology Partners, Inc.
1-6	**State if the system is operational or provide the expected launch date:**	Expected to launch in November of 2022 or later
1-7	**System's security categorization:**	Moderate
1-8	**Date of most recent Security Assessment and Authorization (SA&A) or why one is not required:**	Currently going through its first Security Assessment.
1-9	**Approximate number of individuals with PII in the system:**	Webgrants will hold monitoring information for approximately 500 organizations in a year, depending on the capacity of AmeriCorps Office of Monitoring (OM) and the number of grants selected for monitoring activities. Only organizations that had received AmeriCorps members (Members) and/or financial resources including project sponsors (Project Sponsor) and grantees (Grantee) from AmeriCorps are subject to the monitoring of OM. Information for at least one authorized point of contact for each Project Sponsor and Grantee will be included in Webgrants. The PII about additional individuals associated with each Project Sponsor and Grantee (e.g., employees, Members, volunteers) may be included depending on what is needed to appropriately monitor grant compliance for that organization

3- SIGNATURES (ORIGINAL MAINTAINED BY CHIEF PRIVACY OFFICER)			
	Role	*Signature*	*Date*
3-1	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.**
	This is the first PIA for the system.
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 <u>Not Applicable</u>.**
	Not Applicable

5- SYSTEM PURPOSE	
5-1	**Describe the purpose of the system.**
	OM is responsible for monitoring and testing all AmeriCorps Project Sponsors and Grantees to ensure their activities comply with the Federal regulations and AmeriCorps policies, as well as tracking and resolving any noncompliance concerns, and communicating those findings to the relevant parties. To support the broad range of monitoring activities and enhance the monitoring processes for a wide-spectrum of various grants, projects, and award recipient organizations, OM procures subscription-based WebGrant service from Dulles Technology Partners, Inc. OM will use WebGrant to (1) track all OM monitoring activities and related action items (e.g., when to communicate with a Grantee); (2) organize the broad range of documents created during the monitoring processes in one central location; (3) help standardize OM’s monitoring protocols for different types of projects and grants; and (4) develop longitudinal data that will be used to assess AmeriCorps’ monitoring system and framework and identify opportunities for enhancement. WebGrant is a web-based full lifecycle comprehensive grants management system with rich and robust features which offers flexible and configurable tables, forms, custom fields, reports, and user dashboards, and the abilities to set up workflows that automate grant management monitoring through stages and maintain user activity history. AmerCorps’s Webgrants will be accessed by authorized staff and its support contractors of OM. There will be an external portal where the points of contact for each Project Sponsor and Grantee will be able to login to access their organizations’ account and records, submit forms and upload documents to OM, review anything they

previously submitted through the portal, and track any requests or assignments from OM.

6- INVENTORY OF PII

6-1 **Provide a list of all the PII included in the system.**

PII may include:

- Names
- Organizational contact information (e.g., email, telephone, address, title)
- State of residence and where in the state they are employed or serving
- National Service Participant Identification (NSPID) Numbers,
- Tax Identification Number
- Payroll and time keeping records
- Criminal history information

The PII are used to appropriately monitor the compliance statues of the Project Sponsors and Grantees of AmeriCorps. The information will be retrieved by the grant numbers of the organization instead of any PII of any individual.

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 categories of individuals include the employees, Members, Volunteers, and other individuals connected to those Project Sponsors and Grantees.

There are approximately 500 Project Sponsors and Grantees a year in Webgrants.

OM cannot estimate exactly who or how many individuals will be included for each Project Sponsor and Grantee because it will depend on their activities, their structure, and how they are monitored. For example, Webgrants will generally have information about the key employees associated with each project or grant; each organization decides whether they want to list the same or different staff for different projects or grants.

8- INFORMATION IN THE SYSTEM

8-1 **For each category of individuals discussed above:**

a. **Describe the information (not just PII) collected about that category.**
b. **Give specific details about any PII that is collected.**
c. **Describe how the information is used.**

Webgrants stores the information needed to evaluate whether Project Sponsors and Grantees have complied with AmeriCorps policies, federal regulations, and the Uniform Guidance issued by the United States Office of Management and Budget, and to correct any noncompliance. This information centers around the organization (e.g., operational and financial management policies and their practices) which might include some PII.

Webgrants will store the name and organizational contact information of a point of contact for each Project Sponsor and Grantee. This PII will be used to manage their access to the Wegbrants portal where they communicate with OM.

Webgrants may store additional PII about any individual associated with a Project Sponsor or Grantee for OM to evaluate whether some activity related to that organization is permitted. The specific PII that is collected and stored, and the number of individuals that the PII is related to, will depend on the monitoring needs on an organization. For example:

- If a Project Sponsor did not comply with a requirement related to a service member, OM would want to document that noncompliance in Webgrants and the documentation might include the member's name, contact information, NSPID Number, and information about their service.
- If a Grantee paid an employee using AmeriCorps' funds before checking that employee's criminal history, Webgrants may store the payroll information for that employee in order to calculate the disallowed costs.
- If a Project Sponsor gives a stipend to a service member who may not have passed their Criminal History Check, Webgrants may store a summary of the crime that caused the Member to fail the check or a record showing that the crime had been expunged. However, the information will only be retrieved by grant number.

Webgrants may also store communications with Project Sponsors and Grantees about the concerns.

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.

PII stored in Webgrants will come from the following sources:

1) One of AmeriCorps' other systems is the Electronic-System for Programs, Agreements and National Service Participants (eSPAN). Staff of prospective and current Project Sponsors and Grantees use an eSPAN module called **eGrants Phase 2/Grantee Portal** (eGrants) to (1) apply for, manage, and provide status reports on their grants and (2) apply for, recruit, manage, and provide status reports on their Members. Some of the PII in eGrants will be

	exported to excelsheets and uploaded into Webgrants by WebGrant staff members. 2) Webgrants will have an external platform where points of contact for each Project Sponsor and Grantee will be able to login and provide information including some contact information to OM. Webgrants gives each Project Sponsor and Grantee the ability to control which of their staff may access the system and provide point of contact account profile information. Where possible, it asks the staff to complete a form instead of uploading an attachment so as to more effectively control what PII may be provided. Webgrants also has the functionality to encrypt specific fields that will contain PII so the PII should not be corrupted or intercepted while being transferred. Some PII in Webgrants comes from the Project Sponsor or Grantee during the course of a monitoring activity. Before that occurs, the organization receives from OM a description of the upcoming activity with a timeframe and a description of the information that will be reviewed. That gives the organization an opportunity to confirm that the information is accurate. The organization can then upload any additional information through the Webgrants portal, which provides a secure means of transfer and allows them to later see what they provided.
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 Not Applicable.**
	There are two situations in which Webgrants may be used in the collection and subsequent storage of PII directly from the individual. First, the points of contact for each Project Sponsor and Grantee staff will have an opportunity to login to a secure Webgrants portal, provide their contact information and any other requested PII about themselves, and later view and provide updates to that PII. Second, OM staff may infrequently request some information directly from an individual for account management or grant monitoring purposes and then transcribe or upload that information into Webgrants; the PII that might be included should not affect the individual and the organization will have an opportunity to verify or refute its accuracy before the organization is negatively affected. The information collected and handled by WebGrant is limited for account management and grant monitoring activities. Only information that is relevant to the specific grant management is collected and used. AmeriCorps has standard security and privacy assessment processes in place. All the safeguards required for this system will be identified, implemented and assessed before the system is formally launched, which is subject to continuous monitoring by the agency.
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>.

In almost all situations, the accuracy or inaccuracy of the PII in Webgrants will affect the organization and not an individual. For example, if an organization does not provide requested project expenditure information to support the payment of someone's salary using funds from a particular grant, the organization is still responsible for paying the individual out of their own funds. Before the organization is affected, they will have opportunity to provide additional evidence to validate or correct the record. If the organization needs assistance in completing the request, OM staff will be available to provide clarification.

AmeriCorps has application and processes to assure the PII that is stored in Webgrants is accurate:

- Most PII in Webgrants has already been collected into eGrants and is therefore transferred from eGrants into Webgrants. eGrants gives each Project Sponsor and Grantee the ability to control which of their staff may access the system and provide PII. Where possible, it asks the staff to complete a form instead of uploading an attachment to more effectively control what PII may be provided. eGrants is also encrypted so the PII should not be corrupted or intercepted while being transferred.
- Some PII in Webgrants comes from the Project Sponsor or Grantee during the course of a monitoring activity. Before that occurs, the organization receives a description of the upcoming activity with a timeframe and a description of the information that will be reviewed. That gives the organization an opportunity to confirm that the information is accurate. The organization can then upload any additional information through the Webgrants portal, which provides a secure means of transfer and allows them to later see what they provided.

A small amount of PII in Webgrants will come through a range of communications with affected parties involved in a grant award who may have some information needed by OM to determine whether a Project Sponsor or Grantee has met all its requirements. OM will work to inform those individuals of the information they need and the importance of making sure that information is accurate.

All individuals associated with one of AmeriCorps' Grantees and Project Sponsors who may have their information stored in Webgrants should be aware that part of the support for their project or grant comes from AmeriCorps and that AmeriCorps may evaluate their organization's activities for compliance.

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. If the system does not implicate the PRA, write Not Applicable.**
	Not applicable; none of the collections will be subject to the PRA.
9-5	**If any collections into the system are subject to an agreement, describe those agreements. If no agreements are relevant, write Not Applicable.**
	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.**
	The following categories of individuals will have access to PII within Webgrants for the following reasons: • OM staff will have access in order to complete their monitor roles. • One point of contact for each Project Sponsor and Grantee will be given access to a portal where they can see anything they have submitted through the portal and any requests and assignments from OM specific to their project. The Project Sponsor/Grantee may request additional/change in access to the system through a formal request form on the OM SharePoint that must be approved by their appointed Monitoring Officer. • AmeriCorps staff within the Office of Information Technology will have intermittent access to help implement and assess the system's privacy and security controls. • Webgrants employees and their contractors will have access in order to maintain the system. Both AmerCorps and Webgrants staff and contractors are given the minimum right of access according to the business needs to complete their work and that level of access is removed once they no longer have a reason to retain it.

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.** **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. Any agreements controlling that PII. **If PII is not shared outside the system, write <u>Not Applicable</u>.**
	Not Applicable

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 technical, physical, and administrative safeguards that protect the PII in the system.**
	AmeriCorps's Webgrants is hosted in an Amazon Web Services (AWS) FedRAMP cloud in the US-East region. The system has a robust set of security policies and procedures including permission-based access controls, uptime monitoring, third-party penetration studies, system maintenance procedures, and plans for potential security incidents. An audit log records activities that occur within the system and are subject to review on a regular basis. A very small number of Webgrants vendor staff will have access to AmeriCorps' information in order to manage the database. These staff are only authorized to access AmeriCorps' WebGrant system after they works for the vendor for at least a year, as required by the WebGrant vendor. In addition, all of the vendor staff and AmeriCoprs staff must complete security and privacy training as part of their orientation process and annually thereafter. AmeriCorps controls which of its staff and contractors will have access to the information in Webgrants. All AmeriCorps staff will have completed an annual security and privacy training and those with higher levels of system access will have completed additional annual training for privileged users. Moreover, they will access the system through single sign-on so they will automatically lose that access when they exit AmeriCorps The information from AmeriCorps eGrant is securely transferred to WebGrants. A point of contact for each Project Sponsor and Grantee will have access to a Webgrants portal so they can securely upload any of their organization's information which is not sensitive PII, and are provided access to Secure File Transfer outside of the Webgrants portal so they can securely send and receive information to and from WebGrant.

AmeriCorps takes measures to ensure the infromation collection is minimized to only what is necessary for the grant compliance monitoring activities. To eliminate potential privacy risk that might arise from the compliance monitoring activities, OM post specific notice of not to provides sensitive personal information such as social security numbers on WebGrant website.

Some of information might be imported from AmeriCorps eGrant system. AmeriCorps adequately notifies the public of the PII collected, used, processed, stored and disclosed by eGrant/eSPAN portal and covered routine uses via the publication of eSPAN PIA and the system of records notice CNCS-04-CPO-MMF-Member Management Files (MMF). For more information, please visit the website of AmeriCorps privacy program at WWW.AmeriCorps.Gov/Privacy. The publication of WebGrant PIA provides more details on the specific data activity of WebGrant system and the specific purpose of the system.

WebGrant is currently undergoing series of security assessments and is subject to continuous monitoring of AmeriCorps, which will ensure that the potential privacy risks and security risks will be appropriately identified, and mitigated for the entire life cycle of the system.

The publication of this WebGrant PIA provides notice to the individuals about the data activities and data privacy safeguards of WebGrant system and the privacy practice of AmeriCorps.

14- DATA ACCURACY, ACCESS, AMENDMENT, AND CONTROL

14-1 **Describe the steps taken to ensure PII is sufficiently accurate, relevant, current, and complete.**

PII is collected when an organization needs to set up account for their point of contact. The points of contact for each Project Sponsor and Grantee staff will have an opportunity to login to a secure Webgrants portal, provide their contact information and any other requested PII about themselves, and later view and provide updates to that PII. OM staff may infrequently request certain information directly from an individual related to a grant award and then transcribe or upload that PII into Webgrants; this PII should not affect the individual and the organization will have an opportunity to verify or refute its accuracy before the organization is negatively affected.

In almost all situations, the accuracy or inaccuracy of the PII in Webgrants will affect the organization and not an individual. For example, if an organization does not provide requested project expenditure information to support the payment of someone's salary using funds from a particular grant, the organization is still responsible for paying the individual out of their own funds. Before the organization is affected, they will have opportunity to provide additional evidence to validate or

	correct the record. If the organization needs assistance in completing the request, OM staff will be available to provide clarification. AmeriCorps has developed software and processes to try and assure the PII that is stored in Webgrants is accurate: • Most PII in Webgrants has already been collected into eGrants and is therefore transferred from eGrants into Webgrants. eGrants gives each Project Sponsor and Grantee the ability to control which of their staff may access the system and provide PII. Where possible, it asks the staff to complete a form instead of uploading an attachment to more effectively control what PII may be provided. eGrants is also encrypted so the PII should not be corrupted or intercepted while being transferred. • Some PII in Webgrants comes from the Project Sponsor or Grantee during the course of a monitoring activity. Before that occurs, the organization receives a description of the upcoming activity with a timeframe and a description of the information that will be reviewed. That gives the organization an opportunity to confirm that the information is accurate. The organization can then upload any additional information through the Webgrants portal, which provides a secure means of transfer and allows them to later see what they provided. A small amount of PII in Webgrants will come through a range of communications with various parties who may have some information needed to determine whether a Project Sponsor or Grantee has met all its requirements. OM will work to inform those individuals of the information they need and the importance of making sure that information is accurate. All individuals associated with one of AmeriCorps' Grantees and Project Sponsors who may have their information stored in Webgrants should be aware that part of the support for their project or grant comes from AmeriCorps and that AmeriCorps may evaluate their organization's activities for compliance.
14-2	**Describe how an individual could view, correct, update, or ask to amend their PII.**
	Apart from the points of contact being able to update their information via the Webgrants portal within a given monitoring cycle, individuals will generally not have access to their own PII in Webgrants or any control over that PII. AmeriCorps is legally required to monitor organizations and Webgrants is specifically used for that purpose. Giving individuals the right to access their information could announce an investigation before it is completed while modifying someone's PII during the course of an investigation could destroy the integrity of the investigation. That said, the PII in Webgrants should not affect the individual and the organization will have an opportunity to verify or refute its accuracy before the organization is negatively affected.

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.**
	The subject of interest of OM is the compliance activity of an organization, not an individual. WebGrant is not a system of records.

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.**
	AmeriCorps is working to assign a retention schedule to these records. Until that occurs, all PII stored in Webgrants like eSPAN will remain indefinitely.

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 Not Applicable.**
	OM does not require SSNs for any monitoring purposes but recognizes that organizations may provide full or partial SSNs as part of their payroll or criminal history information without being requested. For that reason, OM will post warning notice to actively inform individuals not to provide SSNs in situations where they would most likely be offered and work to delete any SSNs which are provided before they are added to Webgrants.

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 Not Applicable.**
	The only interaction between Webgrants and the Project Sponsors and Grantees will be via the Americorps WebGrants online portal where a point of contact for each Project Sponsor and Grantee will be able to securely login and then (a) submit forms and uploads to OM, (b) view anything they previously submitted through the portal, and (c) see any request/assignments from OM. The Americorps Webgrants site is hosted in Amazon AWS cloud in a FedRamp compliant environment. The Webgrants system doesn't link to any third-party

	websites. There are no third-party embedded services within Webgrants. The agency's privacy policy is displayed on the Webgrants login page where it is visible to all users.

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