Privacy Impact Assessment
Telework Application Data App (TADA)
Office of the Chief Information Officer

Version 1.0
08/01/2023

Document Revision History

Date	Version	PIA Name/Description	Author
08/11/2023	1.0	Telework Application Data App Initial Release	Stevens, Mackenzie

Table of Contents

The agency is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below help determine any privacy risks related to the E-Government Act or later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

Name/System/Subsystem/Service Name: Telework Agreement Data App (TADA).

Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform) Microsoft Power Platform.

Date Submitted for review/approval: August 11, 2023.

Note: When completing this PIA do not include any information that would raise security concerns or prevent this document from being made publicly available.

1   Description

1.1 Provide the description of the system/subsystem, technology (i.e., Microsoft Products), program, or other data collections (hereinafter referred to as "project"). Explain the reason the project is being created.

The NRC TADA app is designed to provide staff a secure, flexible, user friendly experience in the electronic submission and approvals of telework agreements which enable staff to leverage maximum telework flexibilities to the extent possible as recommended in MD 10.166, Telework and the Collective Bargaining Agreement, Article 7, "Telework." The TADA empowers stakeholders with a secure, role based, flexible interface to view, submit, approve, and generate reports for analysis in future decision making via a standard web browser.

TADA is a canvas app developed on the Microsoft Power Platform. The app does not use any custom scripts.

Dataverse is the data storage behind the Power Platform that allows the secure management of data.

Please mark appropriate response below if your project/system will involve the following:

☒ PowerApps	☐ Public Website
☐ Dashboard	☐ Internal Website
☐ SharePoint	☐ None
☐ Other	

1.2 Does this privacy impact assessment (PIA) support a proposed new project, proposed modification to an existing project, or other situation? Select options that best apply in table below.

Mark appropriate response.

Status Options	
☒	New system/project
☐	Modification to an existing system/project. *If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.*
☐	Annual Review *If making minor edits to an existing system/project, briefly describe the changes below.*
☐	Other (explain)

1.3 Points of Contact: (*Do not adjust or change table fields. Annotate N/A if unknown. If multiple individuals need to be added in a certain field, please add lines where necessary.*)

	Project Manager	System Owner/Data Owner/ Steward	ISSO	Business Project Manager	Technical Project Manager	Executive Sponsor
Name	Mackenzie Stevens	Gwen Hayden	Consuella Debnam	Tanya Parwani	Mackenzie Stevens	David Nelson
Office/ Division/ Branch	OCIO/SDOD/ ADSB	OCIO/SDOD/ ADSB	OCIO/GEMSD/ CSB	OCHCO/ADHROP /WMBB	OCIO/SDOD/ ADSB	OCIO/SDOD/ ADSB
Telephone	301-415-2718	301-287-0761	301-287-0834	301-287-0730	301-415-2718	

2 Authorities and Other Requirements

2.1 What specific legal authorities and/or agreements permit the collection of information for the project?

Provide all statutory and regulatory authorities for operating the project, including the authority to collect the information; NRC internal policy is not a legal authority. Please mark appropriate response in table below.

Mark with an "X" on all that apply.	Authority	Citation/Reference
☐	**Statute**	
☐	**Executive Order**	
☐	**Federal Regulation**	
☐	**Memorandum of Understanding/Agreement**	
☒	**Other (summarize and provide a copy of relevant portion)**	The telework/alternate work address is captured on the NRC Form 624 in the existing telework approval process.

2.2 Explain how the information will be used under the authority listed above (*i.e., enroll employees in a subsidies program to provide subsidy payment*).

The information will be used to capture the telework/alternate work location of an NRC employee, as its currently captured on the NRC Form 624 in the existing telework approval process. This information will also help in automating the determination of the duty location of the employee.

If the project collects Social Security numbers, state why this is necessary and how it will be used.

TADA does not collect social security numbers.

3 Characterization of the Information

In the table below, mark the categories of individuals for whom information is collected.

Category of individual	
☒	Federal employees
☐	Contractors
☐	Members of the Public (any individual other than a federal employee, consultant, or contractor)
☐	Licensees
☐	**Other**

In the table below, is a list of the most common types of PII collected. Mark all PII that is collected and stored by the project/system. If there is additional PII not defined in the table below, a comprehensive listing of PII is provided for further reference in ADAMS at the following link: PII Reference Table 2023.

Categories of Information			
☒	Name	☐	Resume or curriculum vitae
☐	Date of Birth	☐	Driver's License Number
☐	Country of Birth	☐	License Plate Number
☐	Citizenship	☐	Passport number
☐	Nationality	☐	Relatives Information
☐	Race	☐	Taxpayer Identification Number
☒	Home Address	☐	Credit/Debit Card Number
☐	Social Security number (Truncated or Partial)	☐	Medical/health information
☐	Gender	☐	Alien Registration Number
☐	Ethnicity	☐	Professional/personal references
☐	Spouse Information	☐	Criminal History
☐	Personal e-mail address	☐	Biometric identifiers (facial images, fingerprints, iris scans)
☐	Personal Bank Account Number	☐	Emergency contact e.g., a third party to contact in case of an emergency
☐	Personal Mobile Number	☐	Accommodation/disabilities information
☐	Marital Status	☐	**Other**
☐	Children Information		
☐	Mother's Maiden Name		

3.1 Describe how the data is collected for the project. (i.e., NRC Form, survey, questionnaire, existing NRC files/ databases, response to a background check).

The data is collected in fields under the "General Info" tab of TADA for telework/alternate work location of an employee completing the request.

3.2 If using a form to collect the information, provide the form number, title and/or a link.

The information that is currently collected on the NRC Form 624 for telework/alternate work location will be captured in TADA.

3.3 Who provides the information? Is it provided directly from the individual or a third party.

The NRC employee will provide their telework/alternate work location.

3.4 Explain how the accuracy of the data collection is validated. If the project does not check for accuracy, please explain why.

The street number and name of the address is not validated; however, the city and state are auto populated based on the zip code entered in the field. The street number and name of the address may be validated in a future release.

3.5 Will PII data be used in a test environment? If so, explain the rationale.

No.

3.6 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Although the city and state are auto populated based on the zip code, all required fields for the telework/alternate work location are editable fields before a telework request is submitted.

4   Data Security

4.1 Describe who has access to the data in the project (i.e., internal NRC, system administrators, external agencies, contractors, public).

The telework/alternate work location data is stored in a table in Dataverse secured by data loss prevention policies enabled on the platform (MS Power Platform). The tables are only accessible, via the Power Apps Studio, to application administrators within the security group.

4.2 If the project/system shares information with any other NRC systems, identify the system, what information is being shared and the method of sharing.

TADA does not share information with any other NRC system.

4.3 If the project/system connects, receives, or shares information with any external non-NRC partners or systems, identify what is being shared.

Identify what agreements are in place in the table below.

	Agreement Type
☐	Contract Provide Contract Number:
☐	License Provide License Information:
☐	Memorandum of Understanding Provide ADAMS ML number for MOU:
☐	Other

4.4 Describe how the data is accessed and describe the access control mechanisms that prevent misuse.

The telework/alternate work address is accessed via a report run by authorized users in the Office of the Chief Human Capital Officer or Dataverse tables accessible by application administrators within the security group.

4.5 Explain how the data is transmitted and how confidentiality is protected (i.e., encrypting the communication or by encrypting the information before it is transmitted).

Per Microsoft, the following technologies are used for ensuring the secure transit of data:

- "Transport Layer Security/Secure Sockets Layer (TLS/SSL), which uses symmetric cryptography based on a shared secret to encrypt communications as they travel over the network.

- Internet Protocol Security (IPsec), an industry-standard set of protocols used to provide authentication, integrity, and confidentiality of data at the IP packet level as it's transferred across the network.

- Advanced Encryption Standard (AES)-256, the National Institute of Standards and Technology (NIST) specification for a symmetric key data encryption that was adopted by the US government to replace Data Encryption Standard (DES) and RSA 2048 public key encryption technology."

4.6 Describe where the data is being stored (i.e., NRC, Cloud, Contractor Site).

The data is stored in Dataverse, the native data repository for the MS Power Platform.

4.7 Explain if the project can be accessed or operated at more than one location.

TADA, as well as Power Platform environments, is only accessible to those within the NRC Government Commercial Cloud tenant who are in security groups authorized to access.

4.8 Can the project be accessed by a contractor? If so, do they possess an NRC badge?

TADA can only be accessed by those who are in security groups which have been given access to TADA environments. The only contractors who are in these security groups are those who have a need to scan the app (SOC-AIR contractors).

4.9 Explain the auditing measures and technical safeguards in place to prevent misuse of data.

The telework/alternate work location data is stored in a table in Dataverse secured by data loss prevention policies enabled on the platform (MS Power Platform). The tables are only accessible, via the Power Apps Studio, to application administrators within the security group. Additionally, Dataverse tables have columns to support auditing such as who and when a record was last modified. These controls place proper constraints on the accessibility and modification of the data.

4.10 Describe if the project has the capability to identify, locate, and monitor (i.e., trace/track/observe) individuals.

TADA does not identify, locate, and monitor individuals.

4.11 Define which FISMA boundary this project is part of.

TADA is an app under the Business Application Support System (BASS).

4.12 Is there an Authority to Operate (ATO) associated with this project/system?

Authorization Status	
☐	Unknown
☐	No *If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Organization (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.*
☐	In Progress provide the estimated date to receive an ATO. Estimated date:
☒	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO) Confidentiality-Moderate Integrity- Moderate Availability- Moderate

4.13 Provide the NRC system Enterprise Architecture (EA)/Inventory number. If unknown, contact EA Service Desk to get the EA/Inventory number.

20230004.

5 Privacy Act Determination

5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

	Response
☐	**Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, etc.)**
☐	**List the identifiers that will be used to retrieve the information on the individual.**
☒	**No, the PII is not retrieved by a personal identifier.**
☒	**If no, explain how the data is retrieved from the project.** **The privacy data (telework/alternate work address) is stored in the Form624 master table in Dataverse with records accessible by the ap_Form624Id key.**

5.2 For all collections where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a System of Record Notice (SORN) in the Federal Register. *As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other personal identifier assigned to the individual.*

Mark the appropriate response in the table below.

	Response
☒	*Yes, this system is covered by an existing SORN. (See existing SORNs: https://www.nrc.gov/reading-rm/foia/privacy-systems.html)* *Provide the SORN name, number, (List all SORNs that apply):* *Privacy data captured and stored in TADA is covered under the* OPM/GOVT-1 - General Personnel Records and described at 77 Federal Register 73694 (December 11, 2012) and as subsequently modified as described in more recent Federal Register notices (most recent modification as of the date of this form: 87 Federal Register 5874 (February 2, 2022).
☐	**SORN is in progress**
☐	**SORN needs to be created**
☐	**Unaware of an existing SORN**
☐	**No, this system is not a system of records and a SORN is not applicable.**

5.3 When an individual is asked to provide personal data (i.e., form, webpage, survey), is a Privacy Act Statement (PAS) provided?

A Privacy Act Statement is a disclosure statement required to appear on documents used by agencies when an individual is asked to provide personal data. It is required for any forms, surveys, or other documents, including electronic forms, used to solicit personal information from individuals that will be maintained in a system of records.

Mark the appropriate response.

Options	
☒	**Privacy Act Statement** (<u>Privacy Statement in TADA</u>)
☐	**Not Applicable**
☐	**Unknown**

5.4 Is providing the PII mandatory or voluntary? What is the effect on the individual by not providing the information?

The capture of the telework/alternate work address is required. It is currently captured on the Form 624 PDF and required for accountability of the employee.

6 Records and Information Management-Retention and Disposal

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are **Temporary** (eligible at some point for destruction/deletion because they no longer have business value) or **Permanent** (eligible at some point to be transferred to the National Archives because of historical or evidential significance). Records/data and information with historical value, identified as having a "permanent" disposition, are transferred to the National Archives of the United States at the end of their retention period. All other records identified as having a "temporary" disposition are destroyed at the end of their retention period in accordance with the NARA Records Schedule or the General Records Schedule.

These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR, agencies are required to establish procedures for addressing Records and Information Management (RIM) requirements. This includes strategies for establishing and managing recordkeeping requirements and disposition instructions before approving new electronic information systems or enhancements to existing systems.

The following questions are intended to determine whether the records/data and information in the system have approved records retention schedules and disposition instructions, whether the system incorporates RIM strategies including support for <u>NARA's Universal Electronic Records Management (ERM) requirements</u>, and if a mitigation strategy is needed to ensure compliance.

If the project/system:

- Does not have an approved records retention schedule and/or
- Does not have an *automated* RIM functionality,
- Involves a cloud solution,
- And/or if there are additional questions regarding Records and Information Management - Retention and Disposal, please contact the NRC Records staff at **ITIMPolicy.Resource@nrc.gov** for further guidance.

If the project/system has a record retention schedule or an automated RIM functionality, please complete the questions below.

6.1 Does this project map to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule (NUREG-0910), or NARA's General Records Schedules?

☐	NUREG-0910, "NRC Comprehensive Records Disposition Schedule	
☒	NARA's General Records Schedules	

6.2 If so, cite the schedule number, approved disposition, and describe how this is accomplished.

System Name (include sub-systems, platforms, or other locations where the same data resides)	Employee Compensation and Benefits Records
Records Retention Schedule Number(s)	GRS 2.3 item 010 – Employee relations program's administrative records GRS 2.3 item 040 – Telework/alternate worksite program case files
Approved Disposition Instructions	GRS 2.3 - Item 010 - Temporary. Destroy when 3 years old, but longer retention is authorized if required for business use. GRS 2.3 - Item 040 - Temporary. Destroy when superseded or obsolete or 1 year after end of employee's participation in program, whichever is sooner, but longer retention is authorized if required for business use.
Is there a current automated functionality or a manual process to support RIM requirements? This includes the ability to apply records retention and disposition policies in the system(s) to support records accessibility, reliability, integrity, and disposition.	The initial release will not include an automated script for disposition but is planned for a future release.

Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	A planned automated disposition will be scheduled for a future release.
Disposition of Permanent Records Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions? If so, what formats will be used? **NRC Transfer Guidance** **(Information and Records Management Guideline -** **IRMG)**	No

Note: Information in *Section 6, Records and Information Management-Retention and Disposal,* does not need to be fully resolved for final approval of the privacy impact assessment.

7 Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 requires that agencies obtain an Office of Management and Budget (OMB) approval in the form of a "control number"—before promulgating a paper form, website, surveys, questionnaires, or electronic submission from 10 or members of the public. If the data collection is from federal employees regarding work-related duties, then a PRA clearance is not necessary.

7.1 Will the project be collecting any information from 10 or more persons who are not Federal employees?

No.

7.2 Is there any collection of information addressed to all or a substantial majority of an industry (i.e., Fuel Fabrication Facilities or Fuel Cycle Facilities)?

No.

7.3 Is the collection of information required by a rule of general applicability?

No.

Note: For information collection (OMB clearances) questions: contact the NRC's Clearance Officer. Additional guidance can be found on the NRC's internal Information Collections Web page at: https://intranet.nrc.gov/ocio/33456.

STOP HERE - The remaining pages will be completed by the Privacy Officer, Records Management, and Information Collections Team.

8 Privacy Act Determination

Project/System Name: Telework Agreement Data App (TADA).

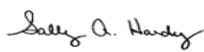**Submitting Office:** IT Services Development and Operations Division (SDOD)

Privacy Officer Review

	Review Results	Action Items
☐	This project/system **does not contain PII.**	**No further action** is necessary for Privacy.
☐	This project/system **does contain PII**; the Privacy Act does **NOT** apply, since information is NOT retrieved by a personal identifier.	**Must be protected with restricted access** to those with a valid need-to-know.
☒	This project/system **does contain PII**; the **Privacy Act does apply**.	**SORN is required-** Information is **retrieved** by a personal identifier**.**

Comments:

Privacy Act Statement is required, and the information is covered by OPM/GOVT-1 - General Personnel Records.

Reviewer's Name	Title
Sally A. Hardy Signed by Hardy, Sally on 08/30/23	Privacy Officer

9 OMB Clearance Determination

NRC Clearance Officer Review

Review Results	
☒	No OMB clearance is needed.
☐	OMB clearance is needed.
☐	Currently has OMB Clearance. Clearance No._____

Comments:

OMB approval is not needed since the information is being collected from current employees of the Federal government acting within the scope of their employment.

Reviewer's Name	Title
[signature] Signed by Cullison, David on 08/28/23	Agency Clearance Officer

10 Records Retention and Disposal Schedule Determination

Records Information Management Review

Review Results	
☐	No record schedule required.
☐	Additional information is needed to complete assessment.
☐	Needs to be scheduled.
☒	Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title
Marna B Dove Signed by Dove, Marna on 08/28/23	Sr. Program Analyst, Electronic Records Manager

11 Branch Chief Review and Concurrence

	Review Results
☐	This project/system **does not** collect, maintain, or disseminate information in identifiable form.
☒	This project/system **does** collect, maintain, or disseminate information in identifiable form.
☒	I concur with the Privacy Act, Information Collections, and Records Management reviews.

Signed by Harris, Kathryn
on 09/06/23

_____

Chief
Cyber Security Branch
Governance and Enterprise Management
  Services Division
Office of the Chief Information Officer

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System: Telework Agreement Data App (TADA).

Date CSB received PIA for review:	**Date CSB completed PIA review:**
August 11, 2023	August 29, 2023

Action Items/Concerns:

Copies of this PIA will be provided to:

Ledetria Beaudoin
Acting Director
IT Services Development and Operations Division
Office of the Chief Information Officer

Garo Nalabandian
Chief Information Security Officer (CISO)
Office of the Chief Information Officer