
U.S. Nuclear Regulatory Commission



Privacy Impact Assessment e-App Office of Administration

**Version 1.0
8/31/2023**

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

Document Revision History

Date	Version	PIA Name/Description	Author
8/31/2023	1.0	e-App PIA - Initial Release.	ADM Oasis Systems, LLC
8/10/2023	DRAFT	e-App PIA - Draft Release.	ADM Oasis Systems, LLC

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

Table of Contents

1	Description	1
2	Authorities and Other Requirements	2
3	Characterization of the Information	3
4	Data Security	5
5	Privacy Act Determination	8
6	Records and Information Management-Retention and Disposal	9
7	Paperwork Reduction Act	11
8	Privacy Act Determination	12
9	OMB Clearance Determination	13
10	Records Retention and Disposal Schedule Determination	14
11	Branch Chief Review and Concurrence	15

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

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: e-App.

Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform): Defense Counterintelligence and Security Agency (DCSA).

Date Submitted for review/approval: August 31, 2023.

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 DCSA National Background Investigation Services (NBIS) e-App system supports the personnel security functions of the NRC Office of Administration (ADM).

e-App is a secure portal, owned and operated by DCSA, designed to house and complete all personnel investigative forms, including the Standard Form SF-85, “Questionnaire for Non-Sensitive Positions”, SF-85P, “Questionnaire for Public Trust Positions,” the SF-85PS, “Supplemental Questionnaire for Selected Positions,” and SF-86, “Questionnaire for National Security Positions”. Individuals are invited into the system electronically to enter, update, and release their personal investigative data over a secure internet connection to their sponsoring agency for review and approval. Once approved, the applicant’s investigative file is submitted by the sponsoring agency to the Investigative Service Provider (ISP) for processing. For NRC usage of e-App, NRC is the sponsoring agency, and DCSA is the ISP.

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

<input type="checkbox"/> PowerApps	<input type="checkbox"/> Public Website
<input type="checkbox"/> Dashboard	<input type="checkbox"/> Internal Website
<input type="checkbox"/> SharePoint	<input type="checkbox"/> None
<input type="checkbox"/> Other:	

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

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	
<input type="checkbox"/>	New system/project
<input checked="" type="checkbox"/>	Modification to an existing system/project. <i>If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.</i> The functionality of DCSA's "Electronic Questionnaires for Investigations Processing (e-QIP)" system has been migrated to the improved e-App system to modernize the application process for personnel background investigation activities. ADAMS ML: ML20288A500
<input type="checkbox"/>	Annual Review <i>If making minor edits to an existing system/project, briefly describe the changes below.</i>
<input type="checkbox"/>	Other (explain)

1.3 Points of Contact:

	Project Manager	System Owner/Data Owner/Steward	ISSO	Business Project Manager	Technical Project Manager	Executive Sponsor
Name	Christoph Heilig	Jennifer Golder	Zia Anderson	N/A	N/A	N/A
Office /Division /Branch	ADM/ DFS/PSB	ADM	ADM/ DRMA/BITT	N/A	N/A	N/A
Telephone	301-415-7731	301-287-0741	N/A	N/A	N/A	N/A

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
<input checked="" type="checkbox"/>	Statute	5 United States Code (U.S.C.) §§ 1103, 1302, 1303, 1304, 3301, 7301, 9101, and 11001; 22 U.S.C. §§ 272b, 290a, and 2519; 31 U.S.C. §§ 1537; 42 U.S.C. §§1874(b) (3), 2165, 2201, and 20132; 50 U.S.C. § 3341; Public Law 108-136; Homeland Security Presidential Directive 12 (HSPD-12); and Section 951 of the "National Defense Authorization Act of Fiscal Year 2018".
<input checked="" type="checkbox"/>	Executive Order	Executive Order (E.O.) 9397 as amended by 13478, 10450, 10577, 10865, 12333, 12968, 13467 as amended, 13488, 13549, and 13869.
<input type="checkbox"/>	Federal Regulation	
<input type="checkbox"/>	Memorandum of Understanding/ Agreement	
<input type="checkbox"/>	Other (summarize and provide a copy of relevant portion)	

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 Federal Government requires background investigations and reinvestigations of all Federal employees, Federal contractors, licensees, applicants, and incumbents. The NRC uses e-App to conduct national security investigations on all of its employees and for personnel that require an NRC clearance.

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

Social Security Numbers (SSNs) are needed to identify records unique to the applicant to support the processing of an applicant's background investigation.

3 Characterization of the Information

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

Category of individual	
<input checked="" type="checkbox"/>	Federal employees
<input checked="" type="checkbox"/>	Contractors
<input checked="" type="checkbox"/>	Members of the Public (any individual other than a federal employee, consultant, or contractor)
<input checked="" type="checkbox"/>	Licensees
<input type="checkbox"/>	Other:

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

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			
<input checked="" type="checkbox"/>	Name	<input checked="" type="checkbox"/>	Resume or curriculum vitae
<input checked="" type="checkbox"/>	Date of Birth	<input type="checkbox"/>	Driver's License Number
<input checked="" type="checkbox"/>	Country of Birth	<input type="checkbox"/>	License Plate Number
<input checked="" type="checkbox"/>	Citizenship	<input checked="" type="checkbox"/>	Passport Number
<input type="checkbox"/>	Nationality	<input checked="" type="checkbox"/>	Relatives Information
<input type="checkbox"/>	Race	<input type="checkbox"/>	Taxpayer Identification Number
<input checked="" type="checkbox"/>	Home Address	<input checked="" type="checkbox"/>	Credit/Debit Card Number
<input checked="" type="checkbox"/>	Social Security Number (Truncated or Partial)	<input checked="" type="checkbox"/>	Medical/health information
<input checked="" type="checkbox"/>	Gender	<input checked="" type="checkbox"/>	Alien Registration Number
<input type="checkbox"/>	Ethnicity	<input checked="" type="checkbox"/>	Professional/personal references
<input checked="" type="checkbox"/>	Spouse Information	<input checked="" type="checkbox"/>	Criminal History
<input checked="" type="checkbox"/>	Personal e-mail address	<input type="checkbox"/>	Biometric identifiers (facial images, fingerprints, iris scans)
<input type="checkbox"/>	Personal Bank Account Number	<input type="checkbox"/>	Emergency contact (e.g., a third party to contact in case of an emergency)
<input checked="" type="checkbox"/>	Personal Mobile Number	<input type="checkbox"/>	Accommodation/disabilities information
<input checked="" type="checkbox"/>	Marital Status	<input checked="" type="checkbox"/>	Other: Education history, employment history, military history, foreign activities/contacts/financial interests, foreign countries visited, police records, drug activity, alcohol use, investigations information, financial information, and civil court actions.
<input checked="" type="checkbox"/>	Children Information		
<input checked="" type="checkbox"/>	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).

Information is collected via an individual's data entry on the electronic forms (SF-85, SF-85P, SF-85PS, and SF-86) in e-App. The NRC, as the hiring agency, then accesses, reviews, and verifies the information, before submitting the completed forms to DCSA for investigation.

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

The following forms are completed in e-App:

- SF-85, "Questionnaire for Non-Sensitive Positions"
- SF-85P, "Questionnaire for Public Trust Positions"
- SF-85PS, "Supplemental Questionnaire for Selected Positions"

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

- SF-86, "Questionnaire for National Security Positions"

Please note, although all the above standard forms are available in e-App, for NRC usage of the system, only the SF-85 and SF-86 are used.

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

Refer to section 3.1.

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

There are numerous checks done within e-App to verify the structure of the data. NRC personnel security initiates a new e-App request for an applicant by inviting them into the system to complete their applicable forms in the system. The applicant completes the forms online, and the system requires each applicant to validate and certify with electronic signature that the form is accurate before submitting it to NRC personnel security. NRC reviews the forms for accuracy and completeness and will reject it back to the applicant if data is missing or requires corrections. If the form is accurate, NRC validates the form within the system and releases the e-App request to DCSA for investigation. If there are validation errors, the system will not allow the form to be submitted.

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

N/A. e-App is owned and operated by DCSA, NRC personnel security and applicants are only users.

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

Applicants are permitted to access e-App only for a limited amount of time in order to complete the required investigative forms. In the event an applicant submitted their forms to NRC and needs to correct inaccurate/erroneous information, they must contact the personnel security team. NRC personnel security will return the form to the applicant for update, recertification, and resubmission to NRC. If the form has already been submitted to DCSA, NRC personnel security will contact DCSA to request that the form be released and returned to the applicant for update, recertification, and resubmission to NRC.

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).

Applicants are invited into the system for a limited period of time to access their investigative data entered into the forms prior to certifying the validity of information. After certification by the applicant, the forms are sent to the NRC personnel security team for review and approval in the system, prior to release to DCSA for investigation.

On the DCSA side, e-App system administrators, security administrators, IT specialists, ISPs, and analysts have access to the system in order to perform their duties in managing, upgrading, and using the system.

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

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.

N/A.

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

e-App is owned and operated by DCSA, NRC personnel security and applicants are only users. The contents of the electronic forms (SF-85, SF-85P, SF-85PS, and SF-86) in the e-App portal are stored and processed by DCSA.

Identify what agreements are in place with the external non-NRC partner or system in the table below.

Agreement Type	
<input type="checkbox"/>	Contract Provide Contract Number:
<input type="checkbox"/>	License Provide License Information:
<input checked="" type="checkbox"/>	Memorandum of Understanding Provide ADAMS ML number for MOU: DCSA NBIS: ML19326A925 DCSA e-QIP*: ML20136A509 <i>*Please note, this agreement has not been updated for the new e-App system.</i>
<input type="checkbox"/>	Other
<input type="checkbox"/>	None

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

Applicants only have access to e-App for a defined period of time to complete the forms; access is removed when the allotted time has expired, or the applicant has certified and released their data. After applicant certification, the forms are sent to the NRC personnel security team for review and approval, prior to release to DCSA for investigation. NRC personnel security staff access is restricted by roles defined and approved for agency users by DCSA.

NRC personnel access is limited only to NRC employee and applicant data within the system. Role-based access controls are employed to limit the access of information by users and administrators based on the need-to-know the information for the performance of their official duties. The e-App system enforces separation of duties, preventing unauthorized disclosure or modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system.

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).

Applicants access e-App over secure (HTTPS) Internet connection. NRC personnel security staff access the system from the NRC VPN.

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

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

Information in e-App is stored by DCSA.

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

DCSA, as the system owner, controls which agencies can access the system. NRC utilizes this system at NRC HQ, the applicant individuals may access this system wherever the internet can be accessed.

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

Yes, all NRC contractors accessing e-App are NRC badged personnel.

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

There are built-in audit logs to monitor disclosures and determine who had access to the forms. The audit log tracks to whom the form is assigned at each step in the process. These logs are checked regularly to ensure that the system is accessed appropriately.

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

N/A.

4.11 Define which FISMA boundary this project is part of.

e-App is an included service under the ADM External Services (AES) subsystem of the Moderate ADM Support System (MASS) FISMA boundary.

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

Authorization Status	
<input type="checkbox"/>	Unknown
<input type="checkbox"/>	No <i>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.</i>
<input type="checkbox"/>	In Progress provide the estimated date to receive an ATO. Estimated date:
<input checked="" type="checkbox"/>	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO) Confidentiality – Moderate Integrity – Moderate Availability – Moderate

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

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

EA Number: 20000307.

5 Privacy Act Determination

5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

Response	
<input checked="" type="checkbox"/>	Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, etc.)
<input checked="" type="checkbox"/>	List the identifiers that will be used to retrieve the information on the individual. Information is retrieved from e-App by name, SSN, or Investigation Request number.
<input type="checkbox"/>	No, the PII is not retrieved by a personal identifier. If no, explain how the data is retrieved from the project.

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	
<input checked="" type="checkbox"/>	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): NRC-39 – "Personnel Security Files and Associated Records" DUSDI 02-DoD – "Personnel Vetting Records System" 83 FR 52420
<input type="checkbox"/>	SORN is in progress
<input type="checkbox"/>	SORN needs to be created
<input type="checkbox"/>	Unaware of an existing SORN
<input type="checkbox"/>	No, this system is not a system of records and a SORN is not applicable.

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

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	
<input type="checkbox"/>	Privacy Act Statement:
<input type="checkbox"/>	Not Applicable
<input checked="" type="checkbox"/>	Unknown N/A – e-App is owned by a non-NRC agency (DCSA).

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

PII disclosure is mandatory, required to identify records unique to the individual for the purpose of the applicant’s background investigation. Additionally, e-App is configured such that if an applicant does not provide an answer to a question, the system will not allow them to proceed with the application until completed.

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 [NARA’s Universal Electronic Records Management \(ERM\) requirements](#), and if a mitigation strategy is needed to ensure compliance.

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

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?

<input type="checkbox"/>	NUREG-0910, “NRC Comprehensive Records Disposition Schedule”
<input checked="" type="checkbox"/>	NARA’s General Records Schedules
<input type="checkbox"/>	Unscheduled

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)	e-App
Records Retention Schedule Number(s)	GRS 5.6 item 180 – Personnel security and access clearance records. Records of people not issued clearance. GRS 5.6 item 181 - Personnel security and access clearance records. Records of people issued clearances.
Approved Disposition Instructions	GRS 5.6 item 180 – Temporary. Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use. GRS 5.6 item 181 – Temporary. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if
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.	N/A
Disposition of Temporary Records	N/A

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	
<p>Disposition of Permanent Records</p> <p>Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions?</p> <p>If so, what formats will be used?</p> <p>NRC Transfer Guidance (Information and Records Management Guideline - IRMG)</p>	N/A

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 more 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?

Yes, the following forms collect information on individuals who are not Federal employees, and are completed in e-App:

- SF-85, "Questionnaire for Non-Sensitive Positions" (OMB No. 3206-0261)
- SF-85P, "Questionnaire for Public Trust Positions" (OMB No. 3206-0258)
- SF-85PS, "Supplemental Questionnaire for Selected Positions" (OMB No. 3206-0258)
- SF-86, "Questionnaire for National Security Positions" (OMB No. 3206-0005)

Please note, although all the above standard forms are available in e-App, for NRC usage of the system, only the SF-85 and SF-86 are used.

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>.

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

8 Privacy Act Determination

Project/System Name: e-App

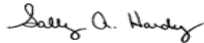
Submitting Office: Office of Administration (ADM)

Privacy Officer Review

Review Results		Action Items
<input type="checkbox"/>	This project/system does not contain PII.	No further action is necessary for Privacy.
<input type="checkbox"/>	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.
<input checked="" type="checkbox"/>	This project/system does contain PII ; the Privacy Act does apply.	SORN is required- Information is retrieved by a personal identifier.

Comments:

Covered by System of Records Notice NRC-39 – “Personnel Security Files and Associated Records”.

Reviewer's Name	Title
 Signed by Hardy, Sally on 12/29/23	Privacy Officer


9 OMB Clearance Determination

NRC Clearance Officer Review

Review Results	
<input type="checkbox"/>	No OMB clearance is needed.
<input type="checkbox"/>	OMB clearance is needed.
<input checked="" type="checkbox"/>	Currently has OMB Clearance. Clearance No. 3206-0261, 3206-0258, 3206-0258, and 3206-0005

Comments:


On 11/15/23, OMB approved the Personnel Vetting Questionnaire (3206-0279) which will replace OPM forms SF86, SF 85P, SF 85P-S, SF 85).

Reviewer's Name	Title
 <p>Signed by Cullison, David on 12/15/23</p>	Agency Clearance Officer

10 Records Retention and Disposal Schedule Determination Records Information Management Review

Review Results	
<input type="checkbox"/>	No record schedule required.
<input type="checkbox"/>	Additional information is needed to complete assessment.
<input type="checkbox"/>	Needs to be scheduled.
<input checked="" type="checkbox"/>	Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title
 Signed by Dove, Marna on 12/20/23	Sr. Program Analyst, Electronic Records Manager

11 Branch Chief Review and Concurrence

Review Results	
<input type="checkbox"/>	This project/system does not collect, maintain, or disseminate information in identifiable form.
<input checked="" type="checkbox"/>	This project/system does collect, maintain, or disseminate information in identifiable form.
<input checked="" type="checkbox"/>	I concur with the Privacy Act, Information Collections, and Records Management reviews.



Signed by Feibus, Jonathan
on 12/29/23

Chief Information Security Officer
Chief Information Security Division
Office of the Chief Information Officer

e-App	Version 1.0
Privacy Impact Assessment	8/31/2023

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System: e-App	
Date CISD received PIA for review: August 31, 2023	Date CISD completed PIA review: December 21, 2023
Action Items/Concerns: 	
<p><i>Copies of this PIA will be provided to:</i></p> <p><i>Caroline Carusone</i> <i>Director</i> <i>IT Services Development and Operations Division</i> <i>Office of the Chief Information Officer</i></p> <p><i>Garó Nalabandian</i> <i>Deputy, Chief Information Security Officer (CISO)</i> <i>Office of the Chief Information Officer</i></p>	