Privacy Impact Assessment for the VA IT System called:

VIC Benefits Discount Card (BDC)

Veterans Affairs Central Office (VACO)

Veterans Experience Office

eMASS ID #1149

Date PIA submitted for review:

05/31/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lynn Olkowski	OITPrivacy@va.gov Lynn.Olkowski@va.gov	202-632- 8405
Information System Security Officer (ISSO)	Anthony Gulbis	Anthony.Gulbis@va.gov	208-429-2245 w. 208-713-4648 c
Information System Owner	Angela Gant-Curtis	Angela.Gant-Curtis@va.gov	540-760-7222

Abstract

The abstract provides the simplest explanation for "what does the system do?".
The Veteran Identification Card (VIC) Benefits Discount Card (BDC) system will allow Veterans to request and receive a general-purpose identification card to demonstrate the status of the Veteran without having to carry and use discharge papers. The Veteran Identification Card (VIC) Benefits Discount Card (BDC) Assessing is a centralized system developed under the Office of Information and Technology to implement the Congressional mandate requiring VA to provide a general-purpose identification card to Veterans. Veterans Identification Card Act 2015, Public Law 114-31, 38USC 5701, will be fulfilled using this system.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?
Veterans Identification Card Benefits Discount Card (BDC-VIC) – Veterans Experience Office

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
Veterans Identification Card Benefits Discount Card (BDC-VIC) system will allow Veterans to request and receive a general-purpose identification card to demonstrate the status of the Veteran without having to carry and use discharge papers. The Veteran Identification Card (VIC) Benefits Discount Card (BDC) is a centralized system developed under the Office of Information and Technology to implement the Congressional mandate requiring VA to provide a general-purpose identification card to Veterans. Veterans Identification Card Act 2015, Public Law 114-31, 38USC 5701, will be fulfilled using this system.

C. Who is the owner or control of the IT system or project?
VIC BDC system owner. VIC BDC is a containerized system within the VA Platform One environment.

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?
Veterans Identification Card Benefits Discount Card (BDC-VIC) system will store information received for eligible Veterans that request the identification card. The number of Veterans whose information stored in the system could be one million or more.

E. *What is a general description of the information in the IT system and the purpose for collecting this information?*

Veterans Identification Card Benefits Discount Card (BDC-VIC) system collects character of discharge documentation to determine eligibility for the identification card. The branch of service, email address, mailing address, government issued identification and a photo are also collected in the system for use with approving the request for the identification card.

F. *What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.*

Information is shared between Veterans Identification Card Benefits Discount Card (BDC-VIC) system and VA Profile to determine eligibility.

G. *Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?*

The system is hosted in VA Enterprise Cloud, and containerized in VA Platform One. All components and data are hosted there. That is the only site.

3. Legal Authority and SORN

H. *What is the citation of the legal authority to operate the IT system?*

Veterans Assistance Discharge Program.

45VA21 - Veterans Assistance Discharge System – VA. govinfo.gov/content/pkg/FR-2023-02-06/pdf/2023-02388.pdf SORN Title and a link to the SORN from the OPRM site. (2010-25233.pdf (govinfo.gov)).

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The SORN does not require amendment or revision and approval. The SORN covers cloud usage and storage.

4. System Changes

J. *Will the completion of this PIA will result in circumstances that require changes to business processes?*

No changes to business processes are required as a result of completing the PIA.

K. *Will the completion of this PIA could potentially result in technology changes?*

No technology changes needed

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

☒ Name
□ Social Security Number
□ Date of Birth
□ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
□ Personal Fax Number
☒ Personal Email Address
□ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
□ Financial Information
□ Health Insurance Beneficiary Numbers Account numbers
□ Certificate/License numbers[1]
□ Vehicle License Plate Number
□ Internet Protocol (IP) Address Numbers
□ Medications
□ Medical Records
□ Race/Ethnicity
□ Tax Identification Number
□ Medical Record Number
□ Gender
☒ Integrated Control Number (ICN)
☒Military History/Service Connection
□ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: *Electronic Data Interchange Personal Identifier, Title 38 Code, Character of Discharge, Branch of Service, Disability Status, and Disability Percentage, VA Email, Work Phone Number, Workload System Username, Non-Identifiable Group Member ID.*

PII Mapping of Components (Servers/Database)

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

VIC BDC consists of 1 key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
VIC BDC Database	**Yes**	**Yes**	**Veteran Name** **Veteran Mailing Address** **Veteran Phone Number** **Veteran email Address** **Electronic Data Interchange Personal Identifier (edipi)** **Character of Discharge** **Branch of Service** **Integration Control Number (ICN)** **Title 38 Code** **Disability Status** **Disability Percentage**	**To determine eligibility and approve request for ID card**	**Hosted in VA environment, controlled physical and logical access, only approved and authorized users granted access.**

1.2 What are the sources of the information in the system?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Information collected directly from Veterans. Information also provided by other VA systems, Identity and Access Management (IAM) and VA Profile.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.
Information is required from Identity and Access Management for Veteran to access the system. Information is required from VA Profile to determine eligibility.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

VIC BDC creates a digital general purpose identification care.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?
Information is collected from Identity and Access Management system for use with granting access to Veterans Identification Card Benefits Discount Card (BDC-VIC) system. Information is collected from VA Profile for determining eligibility for the identification card. Both systems provide identification verification of the Veterans. Otherwise the Veteran would need to provide directly.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

The information is not on a form

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

All information will be collected from the Veteran and is considered accurate. Identity and Access Management (IAM) AccessVA, web portal validate identity using ID.me or Login.gov and grants access to Veterans that allow transactions to be initiated and submitted for processing. VA.gov and IAM AccessVA integrate with the Master Veteran Index (MVI) as part of the identity management and user authorization process. Information received and displayed from other VA systems is considered accurate. Veterans have the ability to validate their personal information and change it as part of completing the request for an identification card. Veterans will be provided the option of using the updated personal information in other VA systems for receiving services and benefits from VA.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

The system does not check for accuracy by accessing a commercial aggregator.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

VIC BDC is developed under –Public Law 114-31; Veteran Information: Title 38, United States Code, Section 5107, Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources. "Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled

"Agency Agreements," also known as the "Economy Act." E-government Act of 2002 (44 U.S.C. §208(b)). 38 United States Code 5706. The Secretary will use the public-private partnerships to promote effective implementation of programs related to suicide prevention, caregivers support, homelessness, TBI research, employment, rehabilitation & reintegration, women's health, and other programs that benefit or serve Veterans. 38 USC 2063, 2021, 2022, 1709(b), 1710(a)(b)(c)(e), 1714, 1717, 7303(a), and 7303(c)(d).

VIC BDC is covered under 45VA21 - Veterans Assistance Discharge System – VA. The VIC BDC a centralized system developed under the legal authority of Title 38, United States Code, Section 501. Public Law (PL) 114-31 amended Chapter 57 of title 38, United States Code to require that an identification card be issued to all Veterans that request a card and present a DD-214 or other document that validates service in the military, naval or air service in the Armed Forces of the United States.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

<u>Principle of Purpose Specification:</u> Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: Data collected by the VIC BDC application contains PII, and other sensitive information. Due to the sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result in a significant financial burden to address impact of stolen identity.

Mitigation: VIC BDC ensures strict access to information by enforcing thorough access control and requirements for end users. All roles in VIC BDC will be managed by system administrators and undergo a documented approval process. Access to VIC BDC will be limited to authorized users of the system and will have appropriate credentials for authentication. As part of the access management activities, the highest level of assurance for providing identity along with multi-factor authentication will be used. Additionally, the system will log access and activity.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Full Name	Used to identify and connect Veterans data across different data sources.	Not applicable
Personal Mailing Address	Used to validate identity	Not applicable
Personal Phone Number	Used to validate identity	Not applicable
Personal eMail Address	Used to validate identity	Not applicable

Integrated Control Number	Used to validate identity	Not applicable
Military History/Service	Used to determine eligibility	Not applicable
Title 38 Code	Used to determine eligibility	Not applicable
Electronic Data Interchange Personal Identifier	Used to determine eligibility	Not applicable
Character of Discharge	Used to determine eligibility	Not applicable
Branch of Service	Used to determine eligibility	Not applicable
Disability Status	Used to determine eligibility	Not applicable
Disability Percentage	Used to determine eligibility	Not applicable
VA Email	To create and allow user access to the system.	To create and allow user access to the system.
Work Phone Number	To create and allow user access to the system.	To create and allow user access to the system.
Workload System Username	To create and allow user access to the system.	To create and allow user access to the system.
Non-Identifiable Group Member ID	To create and allow user access to the system.	To create and allow user access to the system.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?
This system does not process or analyze the data submitted. The data provided is used to produce the VIC BDC and update personal information in other VA systems at the Veterans request.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the *individual? If so, explain fully under which circumstances and by whom that information will be used.*

If the Veterans changes their mailing address or phone number in VIC BDC and indicates the information should be used to update their VA Profile, then the information will be shared with the VA Profile system for use by other VA systems and employees to contacting the Veteran.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

Encryption at rest (HW and DB), encryption in transit (TLS 1.2 or higher), role-based access rules, PIV required, identity proofing of clinician for controlled substance prescribing

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

The system doesn't save SSNs.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

Encryption at rest (HW and DB), encryption in transit (TLS 1.2 or higher), role-based access rules, PIV required, identity proofing of clinician for controlled substance prescribing and does not save SSNs.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

<u>*Principle of Transparency:*</u> *Is the PIA and SORN, if applicable, clear about the uses of the information?*

<u>*Principle of Use Limitation:*</u> *Is the use of information contained in the system relevant to the mission of the project?*
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Access to the PII is governed by role-based access rules in the system.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes. The IAM system has documentation on getting a PIV and roles. VIC BDC documentation defines the roles in the system.

2.4c Does access require manager approval?

System administrator and VA employee user requires approval. System administrator access approved by system owner. VA employee user access approved by Veteran Experience Office (VEO) manager.

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes. All components and use of the system are logged and audited.

2.4e Who is responsible for assuring safeguards for the PII?

The system owner, the VEO business manager and VA government employees are all responsible for following the VA's rules of behavior for assuring the proper procedures and actions are taken when accessing a Veterans record in VIC BDC.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is ***retained*** *by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

Veteran Name, Veteran Mailing Address, Veteran Phone Number, Veteran email Address, Electronic Data Interchange Personal Identifier (edipi), Character of Discharge, Branch of Service, Integration Control Number (ICN), and Title 38 Code are retained.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

VIC BDC information is retained permanently to ensure request for digital card is successfully processed and to respond to requests for replacement cards. The Veteran may request to amend information entered into the system by submitting a new request with the correct information for use with obtaining a digital identification card. The information in VIC BDC is retained in accordance with Veterans Benefits record control schedule, 1180.17 Veterans Benefits N1-15-06-2, Item 8. https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes. VIC BDC is covered under 45VA21 - Veterans Assistance Discharge System – VA. The information in VIC BDC is retained in accordance to VA Records Control Schedule, 1180.17 Veterans Benefits N1-a5-06-2, Item 18. https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.3b Please indicate each records retention schedule, series, and disposition authority?

VIC BDC is covered under 45VA21 - Veterans Assistance Discharge System – VA. The information in VIC BDC is retained in accordance to VA Records Control Schedule, 1180.17 Veterans Benefits N1-a5-06-2, Item 18.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.
Only VA staff can perform those actions. All data cached/stored by VIC BDC is deleted upon reaching the deletion timeframes as specified in 3.2. VIC BDC operates on time-based deletion rules that programmatically triggers a clean-up script. This is in accordance with VA Handbook 6500, Data Minimization and Retention, which states VA will retain PII for only as long as necessary to fulfill the specified purpose(s). Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FType=2. When required, this data is deleted from their file location and then permanently deleted from the deleted items, or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.   Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

VIC BDC provides security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and at least annually thereafter via the VA OIT Talent Management System (TMS).

VIC BDC does NOT use PII/PHI for testing information systems or pre-production prior to deploying to production.

VIC BDC awareness training program commences with the VA OIT TMS training, VA Privacy and Information Security Awareness and Rules of Behavior (ROB), number 10176. Following the training, all information system users will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explain how to report incidents. The awareness program is consistent, updated and deployed for all employees regularly.

<u>3.6 PRIVACY IMPACT ASSESSMENT: Retention of information</u>

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

<u>Principle of Minimization:</u> Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

<u>Principle of Data Quality and Integrity:</u> Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: Records must be maintained to be accurate, relevant, timely and complete. The risk to maintaining data within VIC BDC for a longer time period than what is needed or required is that the longer information is kept, the greater the risk that information will be compromised, unintentionally released or breached.

Mitigation: Access to the system is governed by a need to know. All those with access have been trained in Privacy and Information Security. VIC users are granted access to the system based on approval from the VIC Program Manager. VIC users access the system via Identity Access Management Single Sign-on credentials

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA.gov	Information is received to identify the Veteran, grant access to the system, help determine eligibility and process request for card.	Veteran Name Veteran Mailing Address Veteran Phone Number Veteran email Address Electronic Data Interchange Personal Identifier (edipi) Character of Discharge Branch of Service	SOAP over HTTPS using SSL encryption and Certificate exchange - SSOe
IAM AccessVA	Information is received to identify the Veteran, grant access to the system, help determine eligibility and process request for card.	Veteran Name Veteran Address Veteran Phone Number Veteran Email Address Integration Control Number (ICN) Electronic Data Interchange Personal Identifier (edipi)	SOAP over HTTPS using SSL encryption and Certificate exchange - SSOe
VA Profile	Information is received to help determine eligibility and process request for card.	Title 38 Code, Disability Status	RESTful web service using SSL encryption and Certificate exchange
Individual Veterans	Information provided for use with determining eligibility	Discharge documents (if verification cannot be validated by other means)	Image uploaded to VIC application utilizing HTTPS.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The risk of use of this privacy sensitive system is that it collects, processes, or retains information on Veterans and/or dependents. Unauthorized disclosure could cause harm to Veterans.

Mitigation: Existing mitigation techniques such as access control, auditing and identification authentication are used to protect privacy from internal sharing and disclosure risks, such as trainings, will suffice as mitigation, since there is no increased risk. Risk increases with the number of people having access to protected information.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: N/A There is no longer a required MOU/ISA and no external sharing.

Mitigation: N/A There is no longer a required MOU/ISA and no external sharing.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Yes. Notice is provided to Veteran upon entering any information into VA.gov and VIC BDC. It reinforces to the user that any information they enter into form-fields on the application will be collected. Please see Appendix A for an example. Also, notice is provided within this PIA and the governing SORN VIC BDC 45VA21 - Veterans Assistance Discharge System – VA. Federal Register / Vol. 75, No. 193 / Wednesday, October 6, 2010 / Notices
2023-02388.pdf (govinfo.gov)

This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Privacy information included on VA.gov website. https://www.va.gov/privacy-policy/

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Privacy information included on VA.gov website. https://www.va.gov/privacy-policy/

.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.
Yes, the Veteran has the right to decline. To become eligible for the VIC BDC, the Veteran must apply. There is no penalty for a Veterans refusal; however, we will be unable to supply a VIC BDC without an application. Information is required to determine eligibility. Providing information is a basic assumption and requirement of any application, as an application is by definition a collection of information in order to determine eligibility.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

VIC BDC: The individual has the right to consent as outlined within the System of Records Notice (168VA10P2). All requests must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA address outlined.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

<u>Privacy Risk:</u> There is a risk that the Veterans' who provide information to VA.gov, as mentioned above, will not know how their information is being stored in VIC BDC.

<u>Mitigation:</u> A disclaimer will be placed on the VIC landing page outlining the scope of information usage and retention. A FAQ will be added, and if need be, a notice will be published within the PIA and applicable SORN.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Veterans can access their information using VA.gov or AccessVA. Veterans select a credential service provider to use with VA.gov or AccessVA. The available credential service providers are DS Logon, MyHealtheVet or ID.me. After completing the login to VA.gov or AccessVA using their credential service provider, the Veteran selects VIC from list of available systems. The Veteran is then passed to VIC from VA.gov or AccessVA along with their identifying information and address.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The system is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

The system is not exempt from the access provisions of the Privacy Act.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans can update address, email, phone number and branch of service directly in VIC BDC. Veteran can update name by submitting official document showing name change in VIC BDC.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that *even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

If a Veteran has questions pertaining to data submitted to the VA to obtain services, they will follow standard Amendment processes listed within the SORN and this PIA.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
The system will allow user to enter correct information and request another identification card.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is some risk of inaccurate information being sent to VIC BDC as a result of a Veteran entering incorrect data into VA.gov.

Mitigation: Individuals are provided notice of how to access, redress and correct information maintained in a VBA system of record within the applicable SORN and the PIA. We will monitor user feedback, as well as analyze system data for error rates. Any inaccuracies will be addressed immediately by Veteran either making changes to the information that was entered or by contacting the Veteran via letter sent using the United States Postal Service informing that the request could not be completed because erroneous information was submitted. Section 8. Technical Access and Security.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?
VIC BDC will be using 2 factor authentication mechanism to allow users internal to the VA to access the system (e.g., using Personal Identity Verification PIV). We will be limiting access to only a small set of trusted developers approved to work with and diagnose production issues. Secure Shell (SSH) access will be logged and monitored

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?
There are no users from other agencies that have access to this system.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.
Veterans users can update information. VA employees working in the VEO office review and approve requests for the digital card. System administrators make changes to code and databases so the system remains operational.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.
Contractors will be given access to hosting environment and complete their contractual obligations for ensuring the architecture, and hardware are available; and complies with VA OI&T policy. Contractors will not have access to PII or data contained in the system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.
No additional privacy or security training would be offered specific to the VIC BDC application. Existing VA privacy and PII trainings are deemed to be sufficient.
VA awareness training program commences with the VA OIT TMS training, *VA Privacy and Information Security Awareness and Rules of Behavior (ROB), number 10176.* Following the training, all information system users will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explain how to report incidents. The awareness program is consistent, updated and deployed for all employees regularly.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

In Progress

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date: May 25, 2023*
3. *The Authorization Status: Yes*
4. *The Authorization Date:* July 26, 2023
5. *The Authorization Termination Date:* July 25, 2025
6. *The Risk Review Completion Date:* July 05, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

VA Enterprise Cloud Amazon Web Service (AWS)/VA Platform One (VAPO)

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

N/A

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

None

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Lynn A Olkowski Digitally signed by Lynn A Olkowski
Date: 2024.07.12 13:34:26 -05'00'

Privacy Officer, Lynn Olkowski

ANTHONY GULBIS Digitally signed by ANTHONY GULBIS
Date: 2024.07.10 09:24:42 -06'00'

Information System Security Officer, Anthony Gulbis

ANGELA GANT-CURTIS Digitally signed by ANGELA GANT-CURTIS
Date: 2024.07.12 13:27:34 -05'00'

Information System Owner, Angela Gant-Curtis

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices