Visitor Access Control System-Domestic (VACS-D)

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of system: Visitor Access Control System-Domestic

(b) Bureau: Diplomatic Security

(c) System acronym: VACS-D

(d) iMatrix Asset ID Number: 876

(e) Reason for performing PIA:

☐ New system

☒ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

As described in the Notification of Planned Significant Change dated January 8, 2014, a number of peripheral devices have been added to the system boundary, which constituted a signification change requiring a targeted security assessment.

In addition, the latest approved PIA for VACS-D is dated July 13, 2009; it must be updated to come back into compliance with the requirements of legal, regulatory, and Department policy.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
Assessment and authorization (A&A) has begun and is expected to be granted around June of 2016.

(c) Describe the purpose of the system:

VACS-D is an automated visitor registration application that is used to pre-register visitors to designated Department of State (DoS) facilities via OpenNet and to print temporary visitor identification badges when the visitor arrives. Before a visitor's arrival at the DoS facility, the visitor's sponsor can enter the visitor's identification information in VACS-D. When the visitor arrives, the receptionist can print a standard, temporary identification badge after verifying the visitor's identification. The application also provides a report mechanism that the Bureau of Diplomatic Security (DS) uses to monitor visitor access in support of mission requirements to protect domestic DoS facilities from unauthorized access.

VACS-D is currently installed in the following designated DoS domestic facilities:

- Harry S Truman (HST) building, located in Washington, DC
- United States Mission to the United Nations (USUN), located in New York City, NY
- State Annex (SA) 20, Rosslyn, VA
- SA-17, Washington, DC

VACS-D supports Office of Domestic Facilities Protection (DS/DO/DFP) mission requirements to control visitor access to Department of State domestic facilities; provide expertise in response to the Bureau of Diplomatic Security's (DS) mission to investigate violations of the law involving United States passports and visas; protect the Secretary of State and visiting foreign dignitaries; and provide security for DoS domestic facilities.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The PII that is collected, used, maintained, and disseminated consists of the visitor's name; date of birth; and proof of identity documentation, type, and number. A visitor's social security number (SSN) is captured only if it appears on the identification that the visitor presents for access. One example is a state driver's license that uses the SSN as the driver's license number.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

The legal authority for the collection of information is the same as that which established the Bureau of Diplomatic Security: The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Pub. L. 99-399; 22 U.S.C. 4801, et seq. (1986)) as amended. This legislation is cited in 12 Foreign Affairs Manual (FAM) 012, Legal Authorities.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

Info searchable is by name only.

SORN Name and Number: STATE-36, Security Records, May 9, 2013

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number: A-11-014-32: Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11: Visitor Access Control System (Domestic) (VACS(D))
- Length of time the information is retained in the system: Records of access are destroyed when 5 years old unless retained for specific ongoing security investigation.
- Type of information retained in the system:
Visitor access records to specific Department of State buildings

- Schedule number: A-11-014-33: Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11: Visitor Access Control System (Domestic) (VACS(D))
- Length of time the information is retained in the system: Records are destroyed immediately after data have been entered or otherwise incorporated into the master file or database and verified.
- Type of information retained in the system:
Electronic records entered into the system during an update process, and not required for audit and legal purposes.

- Schedule number: A-11-014-34: Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11: Visitor Access Control System (Domestic) (VACS(D))
- Length of time the information is retained in the system: Records are destroyed when business use ceases.
- Type of information retained in the system:
Electronic files consisting solely of records extracted from a single master file or database that is disposable under GRS 20 or approved for deletion by a NARA-approved disposition schedule, excluding extracts that are produced as an extraction process which changes the informational content of the source master file or database; which may not be destroyed before security before securing NARA approval.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public

☒ U.S. Government employees/Contractor employees

☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐Yes ☒No

The receptionist scans each visitor's identification card into the visitor record. A visitor's social security number (SSN) is captured only if it appears on the identification card that the visitor presents. The SSN is not required to be retained by the VACS(D) system for access into buildings. Example: A visitor presents as identification a state driver's license that uses SSN as the driver's license number.

- If yes, under what authorization?

(c) How is the information collected?

The VACS-D system consists of two methods of data collection. Data is collected by completion of a web-based interface by sponsoring DoS employees using the web-based Pre-registration tool or by DoS receptionists who utilize a client application sign-in tool to input visitor information into VACS-D. Data is received from an official visitor ID.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?

Information is verified by receptionists at the each physical location upon arrival of each visitor. Receptionists validate that the information entered into the VACS-D system correctly corresponds with the type and form of identification provided by both the visitor and the escort authority.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

The information is as current as the information received from the data sources. Information is obtained by government-issued IDs.

(g) Does the system use information from commercial sources? Is the information publicly available?

The system does not use any commercial information, publicly available information or information from other Federal agency databases. System information is derived from visitors seeking entrance to specific Department of State buildings.

(h) Is notice provided to the individual prior to the collection of his or her information?
Notice of the purpose, use and authority for collection of information submitted are described in the System of Records Notices titled STATE-36, Security Records. Additionally, a Privacy Act Statement is provided at the logon point of the VACS-D web form, warning users that PII is collected and of its uses.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?
Individuals are asked for their information; if they decline to provide it, they will be denied access to the facility.
- If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?
Privacy concerns influenced the type of information collected by ensuring only necessary items are included to balance security and privacy needs. The system is designed to collect as little PII as possible to function.

5. Use of information

(a) What is/are the intended use(s) for the information?
The information is collected and maintained for the purpose of validating the identity of visitors and for managing visitor logs to maintain the safety and security of Department of State facilities.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes, the system was designed to register visitors arriving to Department of State government sites. Information from government-issued IDs is required to access the agency.

(c) Does the system analyze the information stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the information?
Analysis of the information is limited to non-subject-based statistical information, such as the number of visitors received by Department sites. System generated reports and previous visits are data elements that are part of the data analysis.

(2) Does the analysis result in new information?
The minimal analysis does not result in new information about the individuals.

(3) Will the new information be placed in the individual's record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☒No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
N/A: The VACS-D application does not interface, connect, or interconnect with other systems to share data internally and/or externally with other applications, systems or networks.

(b) What information will be shared?
N/A: The VACS-D application does not interface, connect, or interconnect with other systems to share data internally and/or externally with other applications, systems or networks.

(c) What is the purpose for sharing the information?
N/A: The VACS-D application does not interface, connect, or interconnect with other systems to share data internally and/or externally with other applications, systems or networks.

(d) The information to be shared is transmitted or disclosed by what methods?
N/A: The VACS-D application does not interface, connect, or interconnect with other systems to share data internally and/or externally with other applications, systems or networks.

(e) What safeguards are in place for each internal or external sharing arrangement?
N/A: The VACS-D application does not interface, connect, or interconnect with other systems to share data internally and/or externally with other applications, systems or networks.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
N/A: The VACS-D application does not interface, connect, or interconnect with other systems to share data internally and/or externally with other applications, systems or networks.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Privacy Act and/or Freedom of Information Act (FOIA) requests to the Department of State are required to gain access to information.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

If an individual needs to make a change, they would make the request to the VACS-D user verbally only. The individual wanting the change cannot make the changes themselves. The authorized user would make the changes into the VACS-D system on behalf of the requesting individual.

If no, explain why not.

N/A

(c) By what means are individuals notified of the procedures to correct their information?

Individuals are notified of procedures at time of visitation to DOS facility verbally by reception personnel or host.

8. Security Controls

(a) How is the information in the system secured?

The VACDS-D application is accessed via OpenNet using DoS configured type OpenNet workstations. Authorized users must first authenticate to OpenNet using their OpenNet user ID and password before accessing VACS-D.

The two methods of accessing the application are: 1) Client-based access for receptionists; and, 2) OpenNet intranet web-based access for visitors. Receptionists access the application via the PassagePoint client installed on type OpenNet workstations installed at designated Department domestic facility entrances. The workstations and client software are maintained by the Bureau of Information Resource Management (IRM) and are not considered part of the system boundary. In order to access the application, a receptionist must be granted access in either a Windows active directory (AD) account, which is controlled by the "Security Group DS-VACS" group that is managed by Systems Management Division, Operations Branch (DS/CTO/SMD/OPS), or a user account, which is created within the VACS-D application by DS/CTO/SMD/OPS.

Non-production uses (e.g., testing, training) of production data are limited by administrative controls. Diplomatic Security uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor the OpenNet-connected systems that host DS's major and minor applications, including the VACS-D components, for changes to the DoS mandated security controls. Access controls are in place for the back-end Oracle database, which are based upon role-based permissions configured for "least privilege". The review process establishes segregation of duties for the application.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

User access to the VACS-D system is restricted to authorized DoS staff and contractor employees. The application and database administrators are the only users with elevated privileged access to the database, and only for purposes of system administration and maintenance. All access to the application system is enforced by user profiles according to the principle of least privilege and the concept of separation of duties. The security controls are required in accordance with NIST SP 800-53, Rev. 4.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

VACS-D is monitored by inherited security controls of the OpenNet general support system. Controls built into OpenNet include routers and Network Intrusion Detection Systems (NIDS). These controls provide network level controls that limit the risk of unauthorized access from all IP segments, to include patch management, configuration management, and segregation of duties. In addition, the application is placed behind a virtual firewall to further limit access to system data.

(d) Explain the privacy training provided to authorized users of the system.

Department users are required to attend a security briefing before access to Department systems is granted. This briefing also includes privacy orientation. Users are also required to complete Cybersecurity Awareness Training on an annual basis and must acknowledge in place policies by signing user agreements. System administrators and privileged users are required to complete a separate security awareness briefing provided by the Information System Security Officer (ISSO) as well as sign an Acknowledgement of Understanding and Rules of Behavior statement.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

Because PII is present in the application, FIPS 140-2 encryption is in place for all sessions. Users are only allowed access to data required for their particular task.

(f) How were the security measures above influenced by the type of information collected?

The VACS-D application system is categorized as a "Moderate" risk system in accordance with FIPS 199. In light of this, NIST SP 800-53, Rev. 4 "Moderate" security controls were applied in accordance with OMB to ensure the security of the application as a whole, including the protection of PII.

9. Data Access

(a) Who has access to data in the system?

There are two (2) groups of users: 1) Employees who process a visitor access request (VAR) at Department domestic locations; and, 2) Receptionists who verify and log the identity of each visitor granted temporary access to designated Department domestic locations.

(b) How is access to data in the system determined?

The VACS-D application is restricted to authorized cleared Department of State direct hire and contractor employees. Only application and database administrators are allowed direct access to the database, and this access is only allowed for purposes of performing scheduled and unscheduled maintenance. Additionally, all access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No Information discussing controls for the system are located in the system security plan and NIST SP 800-53, Rev. 4 controls, which are also part of the system security plan.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Access to VACS-D data is role based and configured within the Oracle 11G database. Least privilege and separation of duties are in place for the system. All users will not have access to all data in the system. PII is restricted to authorized personnel. Access is based upon least privilege controls configured for the IMS-U Oracle 11G database. Users are only allowed to access data required to complete particular tasks.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Access controls are in place for the Oracle 11G databases. Access is based on role-based permissions configured for “least privilege”, which establishes separation of duties. Authentication is established via Windows Authentication using single sign-on via the OpenNet general support system. Only database administrators have access to the VACS-D Oracle database.