DS Daily-C PIA

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: DS Daily-C

(b) Bureau: Diplomatic Security

(c) System acronym: DS Daily

(d) iMatrix Asset ID Number: 258439

(e) Reason for performing PIA: see below

☒ New system

☐ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): N/A

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?
DS Daily-C is undergoing A&A activity, which is expected to conclude June 2020.

(c) Describe the purpose of the system:

The DS Daily-C, Version 01.00.00, iMatrix #258439 application system supports the Bureau of Diplomatic Security (DS)'s mission to provide accurate and timely security-based information via the posting of security-related reports of interest to key Department personnel both overseas and domestically. The DS Daily-C was developed to provide a more efficient editorial workflow for the production of DS intelligence articles and a single, easily accessible location to consolidate intelligence products published and disseminated by DS program offices responsible for assessing threat and security incidents. These products, particularly the Diplomatic Security Daily (DSD), keep DS and other Department of State personnel apprised of issues in global areas of interest and support threat mitigation decision making through the provision of analysis and contextual background related to incidents of terrorism, political violence, and crime. This information is currently made available via e-mail dissemination, on an internal Department SharePoint site, and on an externally facing SIPRNet site accessible by United States (US) Government agencies with a national security mission. The DS Daily-C application is intended to replace the current internal DS Daily SharePoint site and provide a sustainable and searchable archive of the data disseminated via e-mail in PDF format to Department consumers. The DS Daily-C will not be accessible by non-Department of State personnel and is not intended to replace the existing external SIPRNet DS Source application.

This PIA is exclusively about DS Daily-C, the editorial workflow tool.

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

- Names
- Birthdates
- Phone number(s)
- Home addresses
- Images or Biometrics IDs

Based on the content of the source material used in the drafting of the individual reports that will be housed on the DS Daily-C site, the DS Daily-C may contain PII associated with: foreign nationals; members of the American public who are the victims or perpetrators of terrorism, political violence, and/or crime; and US Government employees/contractors who are identified as being directly or indirectly involved in or associated with suspicious activities and/or criminal activity near USG property.

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

- 22 U.S. Code 4802 – Responsibility of Secretary of State
  - 22 U.S.Code 4802 (a)- Security Functions
    - (1) (A)
  - 22 U.S.Code 4802 (a)- Security Functions
    - (2) (B) (iii) – Security and protective operations
    - (2) (C) – Counterterrorism planning and coordination
  - 22 U.S. Code 4082 (b) – Overseas Evacuations

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

☒Yes, provide:

- SORN Name and Number: STATE-36, Security Records

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): June 15, 2018

☐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 (e.g., (XX-587-XX-XXX)): A-11-022-02
- Length of time the information is retained in the system: Data is cut-off at the end of the calendar year of final action. Records are destroyed/deleted when they are 15 years old, but no later than 30 years if required for business use. Repository of record is Department of State front-channel cable, transmitted daily with DS Daily-C content.
- Type of information retained in the system:
  The DS Daily-C application is a web-based application that provides a searchable repository of threat analysis and security information pertaining to terrorist threats and incidents of political violence and crime directed against US interests overseas, as published in the DS Daily-C intelligence product. The purpose of the information is to provide accurate and timely intelligence assessment to key Department personnel both overseas and domestically, to assist with threat mitigation and security resource allocation.

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

- If yes, under what authorization?
The following authorities are broad mandates for agencies to combat terrorism through the sharing of terrorism-related information amongst themselves. The DS Daily-C does not specifically collect SSNs; but SSNs are imbedded within the intelligence products which the Daily-C distributes to others.

- 22 U.S.C. 2712 (Authority to control certain terrorism-related services)
- 18 U.S.C. 112 (Protection of foreign officials, official guests, and internationally protected persons)
- Pub. L. 107-56, 10/26/2001 (USA PATRIOT Act - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)
- Executive Order 13356 (Strengthening the Sharing of Terrorism Information to Protect Americans)

(c) How is the information collected?
Authors manually collect and gather information from various US Government sources.

(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?
All information is derived from Diplomatic Security, Department of State, and other US Government sources/repositories, which are reviewed and approved for accuracy and dissemination by the originating agency prior to review and use in the DS Daily-C application.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
The information is current. Articles are reviewed within 24 hours of submission for publication. If new information relevant to a previously published article is received, an author has the option to submit a revised document for publication in order to update the original information and analysis.

(g) Does the system use information from commercial sources? Is the information publicly available?
The answer is "No" for both questions.

(h) Is notice provided to the individual prior to the collection of his or her information?
The DS Daily-C application does not allow for the direct collection of information from individuals; information in DS Daily-C is derived from data that was previously collected and collated in other USG databases, and in some instances, other Department offices. Individuals are provided notice by those particular sources. In cases where data is sourced from other Department sources/databases, notice would be provided at the point of collection by the office collecting the PII.

(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?

N/A

- If no, why are individuals not allowed to provide consent?

The DS Daily-C is not a collection platform nor a repository for information provided directly by individuals; there is no instance in which the authors and editors of DS Daily-C material will interact with an individual whose information has been collected, so there is no means to provide an option for consent. However, when the data is originally collected it is governed by the legal authorities and/or privacy impact considerations of the collecting body. All information used in DS Daily-C is derived from these primary sources.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

Privacy concerns and the need to protect classified information have therefore dictated the level of access to the information contained on the site. Only those Department employees with need-to-know have access permissions; this includes US citizen direct hire and contract staff. Locally engaged nationals are not granted permission to access the application due to privacy concerns.

5. Use of information

(a) What is/are the intended use(s) for the information?

The DS Daily-C is designed to provide Department leadership and security personnel with ease-of-use and consistent access to both current and archived intelligence analysis pertaining to threats from terrorism and incidents of political violence, in order to support threat mitigation and security resource allocation decision-making.

(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.

(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?

(2) Does the analysis result in new information?

(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.

External Sharing: External information sharing is not in place for DS Daily-C. Entities and agencies external to the Department will not have direct access to the application.

Internal Sharing: Access to the DS Daily-C application is only available to Department personnel with a minimum of a secret-level clearance and a need-to-know pertaining to security-related responsibilities. Current user estimates based on permissions anticipated for Regional Security Officers and DS headquarters staff is approximately 500+ users.

(b) What information will be shared?

Internal Sharing: All information contained in the DS Daily-C intelligence product, to include the information types identified in Section 3 of this document, is provided to end users in the form of published reports generated within the application and made available for review.

(c) What is the purpose for sharing the information?

Internal Sharing: From a user perspective, the DS Daily-C information provides analysis of terrorist threats and incidents of political violence in order to provide critical context and background to those with threat mitigation, countermeasure, and security resource allocation responsibilities.

(d) The information to be shared is transmitted or disclosed by what methods?

Internal Sharing: The published reports, edited and published via the DS Daily-C authoring/editing workflow, will be housed on the DS Daily-C End-user Website, where authorized users will be able to search, select, and review articles and/or publications pertinent to their mission and/or geographic location. Authorized DS Daily-C users are Department employees possessing a minimum of a secret clearance.

(e) What safeguards are in place for each internal or external sharing arrangement?

Access is controlled by virtue of access rights to ClassNet and need to know.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns include ensuring that access to the reports generated by DS Daily-C, which may contain PII, are limited to those with a need to know. By virtue of access rights to ClassNet, this concern has been addressed. The system is located in a classified environment. There are no outside connections to the system. The aforementioned safeguards referenced in 6(e) are appropriate in proportion to the value of the information availability.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Information on individuals stored in the DS Daily-C application is derived from Diplomatic Security, Department of State, and other US Government sources and databases whose legal authorities allow for individuals to access their data stored in the originating repository. In addition, as a security information repository owned by the DS, SORN State-36 discusses exclusions from the access and redress provisions of the Privacy Act that apply to DS Daily-C information in order to prevent harm to law enforcement investigations or interests. Separate from this, an individual requiring access to their information on the DS Daily-C application can make a request via the Freedom of Information Act through Bureau of Diplomatic Security, Office of Freedom of Information Act and Privacy Act (DS/MGT/FOIA-PA).

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

☐Yes ☒No

If yes, explain the procedures.

If no, explain why not.

Since DS Daily-C application data is derived from Diplomatic Security, Department of State, and other US Government sources and databases, the individual’s recourse to correct their information would be through the originating entity rather than through the DS Daily-C. This system is also excluded from amendment procedures under the Privacy Act pursuant to the J2 exemption in the law.

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

DS Daily-C does not provide individuals with any notification procedures to correct information. Any applicable notification procedures are the responsibility of the originating collection/repository. Procedures for notification and redress are published in SORN State 36 and in rules published at 22 CFR 171.31. The procedures inform the individual how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record if permissible. It is noted that records in this system are exempt from the Privacy Act under section J2.

8. Security Controls

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

DS Daily-C relies on the inherent security controls native to DoS ClassNet in addition to the application level access controls. Role-based access controls are in place for the DS Daily-C application system consisting of three (3) role groups. Each role is broken down into specific roles within each group. Applicable access security controls are implemented in accordance with NIST SP 800-53, AND 800-53A.

(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.

Individuals will gain access through Single Sign-on (SSO) via ClassNet, ensuring that users have adequate security clearance level and a valid need-to-know. In addition, the Business Owner for this application is the Threat Investigations and Analysis Directorate (DS/TIA), which will approve and authorize the overall use of the DS Daily-C site by agencies, offices, and others with a need for access to the data. Individual requests for accounts will be vetted by DS direct-hire employees. All collected, published, and disseminated DS Daily-C information is made available only to authorized users with appropriate clearances and need-to-know access in order to satisfy the Department's responsibility to adequately protect classified, national security data.
Adjudicated access to DS Daily-C application privileged functions (deployed in hardware, software, and firmware) and security-relevant information restricts the data that may be seen and the degree to which data may be modified by individual users. A system use notification ("warning banner") is displayed before log-on is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

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

Please see responses to 8(b), above. The DS Daily-C application collects all detailed logs for monitoring, recording, and auditing the system. DS Daily-C is monitored by inherited security controls in place for the ClassNet general support system. Controls are built into ClassNet include routers, and Network Intrusion Detection (NIDS).

(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 a privacy orientation. Users are also required to complete the Cybersecurity Awareness Training course, which contains a module on privacy, 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. Annual "Protecting PII" (PA459) course is required for all Civil Service, Foreign Service and Locally Employed Staff that handle PII.

(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.

Authentication is handled by Single Sign-On (SSO) procedure, information access is controlled by manual owner permission and an Active Security List. Non-production uses (e.g., testing, training) of production data are limited by administrative controls. In addition, the Department uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor ClassNet connected systems that host DS's major and minor applications, including the DS Daily-C components, for changes to the DOS mandated security controls.

(f) How were the security measures above influenced by the type of information collected?
The DS Daily-C contains classified, national security-level information derived from intelligence sources and methods and requires the level of information security native to ClassNet. The PII associated with DS Daily-C is therefore protected at the same level as the classified intelligence information that comprises the majority of the DS Daily-C content.

9. Data Access

(a) Who has access to data in the system?
Authorized users include Administrators, Authors, Editors, and authorized end users who are Department of State personnel possessing a minimum of a secret security clearance.

(b) How is access to data in the system determined?
Access is granted by management and is role based. The DS Daily-C application has four (4) role groups, each containing a set of specific roles within DS Daily-C. The groups consist of Administrator, Author, Editor, and authorized end users. These roles reflect the workflow process required to author, edit, and publish the daily intelligence product; while each role has unique duties and permissions within the system, they are not primarily security-based designations. The PII in DS Daily-C is retrieved for the creation of published articles and all persons with access to the DS Daily-C website are able to read, search, and review the articles. Users whose roles provide access to the back-end authoring, editing, and administrative aspects of the application are able to view PII in draft articles, in addition to the disseminated and published versions that appear on the website.

Below is a list of specific roles within each group
DS Daily-C Roles

- Administrator (Authorizing Site): DS Daily-C role that has the ability to modify user permission levels and specific fields throughout the DS Daily-C application system. This role has access to PII within the DS Daily-C database and access to all draft and published PII contained within the system.
- Author (Authoring Site): DS Daily-C role that consists of the Office of Intelligence and Threat Analysis (ITA) Analysts and other analysts from Intelligence Community who create DS Daily-C articles.
- This role has access to PII within the DS Daily-C database and access to all draft and published PII contained within the system.

- Editor (Authoring Site): DS Daily-C role that consists of ITA editors who review, edit, and publish DS Daily-C articles. This role has access to all draft and published PII contained within the system.
- Authorized End Users (End-User Site): This role represents the Department of State employees who are allowed to view DS Daily articles and reports. This group may include, but not be limited to: DS employees, DS security personnel stationed both domestically and abroad, and/or any Department employee possessing a minimum of a secret security clearance. This role has access to all published PII contained within the system.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

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

All users will not have access to all data in the system. PII is restricted to authorized personnel. Users are only allowed to access data required to complete particular tasks. Access is based upon least privilege controls configured for the DS Daily-C application. Only the System Administrator role and Author role have access to PII data stored in the database. Remaining authorized users have access to draft published PII data required for the generation of documents. Access privileges for all users are listed in the response for question 9b.

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

The EventTracker log monitoring tool is used in the ClassNet environment to monitor system servers. Audit logs are reviewed and managed by the security team to ensure that unauthorized changes are not made to system data by reviewing audit logs generated by the EventTracker tool.