PRIVACY IMPACT ASSESSMENT

DSS Task Tracker – Unclassified (TASKR-U) PIA

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: September 2022
(b) Name of system: DSS Task Tracker - Unclassified
(c) System acronym: TASKR-U
(d) Bureau: Diplomatic Security (DS)
(e) iMatrix Asset ID Number: 291066
(f) Child systems (if applicable) and iMatrix Asset ID Number: Not Applicable (N/A)

(g) Reason for performing PIA:

☒ New system
☐ Significant modification to an existing system
☐ To update existing PIA for a triennial security reauthorization

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

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes
☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes
☐No

(c) Describe the purpose of the system:

The DSS Task Tracker – Unclassified (TASKR-U) is used throughout Diplomatic Security (DS) to provide memorandums, reports, and other essential papers for DS Senior Leadership including the Assistant Secretary (A/S), Principal Deputy Assistant Secretary (PDAS), and Deputy Assistant Secretaries (DAS).

TASKR-U performs three (3) essential functions: (1) Streamlines and standardizes the process for clearing tasks within DS; (2) Enables users to simultaneously collaborate on projects via shared tasks; and (3) Acts as a central archival repository for completed tasks and decisions.

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

TASKR-U may collect the following PII on U.S. government employees, contractors, members of the public, and non-U.S. persons when applicable to the tasker:

- Name
- Personal Phone Number
- Personal Email Address
- Personal Address
- Partial Social Security Number (SSN)
- Full SSN
- Passport Number
- Date of Birth
- Citizenship
- Personnel/Employment
- Work Email
- Work Title
- Work Phone Number
- Work Address

The applicable PII is collected from both U.S. persons and non-U.S.-persons. The remainder of this PIA will focus only on PII of U.S.-persons.

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

- Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 U.S.C. § 4802, as amended;
- Foreign Assistance Act, 22 U.S.C. § 2349aa et. seq.; and
- Social Security Act of 1935

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

☒Yes, provide:

- SORN Name and Number:

Security Records, STATE-36

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  Friday, 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 Office 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 (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):
- Disposition Authority Number:
  See below table.

- Length of time the information is retained in the system:
  See below table.

- Type of information retained in the system:
  See below table.

DoS Records Schedule/Disposition Authority Number	Disposition	Description
Program Support Records Disposition Authority Number: DAA-0059-2018-0003-0006 Applies To: - **DS/C** - **DS/CTS** - **DS/DO** - **DS/DSS** - **DS/EX** - **DS/HTP** - **DS/IP** - **DS/PA** - **DS/SI** - **DS/T** - **DS/TIA**	Temporary. Cut-off at end of calendar year of final action. Destroy/delete 3 years after cut-off but no later than 10 years if required for business use.	Records relating to the support of security and law enforcement programs and initiatives. Records include, but are not limited to, memoranda, memorandum of agreements (MOAs); memorandum of understandings (MOUs); correspondence; congressional request or inquiries; research; policies and procedures; activities, status, or other reports; requirements; surveys; drawings; waivers; plans; studies; and investigations covering accreditation, anti-terrorism, assessments, asset forfeiture, building construction, computer security, counterintelligence, countermeasures, cybersecurity, crisis management, contractors, courier services, debugging, demolition, defensive equipment, Government-owned and commercially leased motor vehicles, electronic security, emergencies covering U.S. citizens abroad, emanations, engineering, inspections, inventories, penetration, physical security, product certification, product evaluation, program reviews, protective detail, security incidents, shielding, special events, surveillance detection, systems development, Tempest, testing, training, travel schedules, zones of control, victim resource advocacy, employee work schedules and assignments, Law Enforcement Availability Pay (LEAP) and other law enforcement personnel related matters, and other related subjects.
Working Files Disp Authority Number: DAA-0059-2018-0003-0010 Applies To: - **DS/C** - **DS/CTS** - **DS/DO** - **DS/DSS** - **DS/EX** - **DS/HTP** - **DS/IP**	Temporary. Cut-off at the end of calendar year. Destroy 3 years after cut-off but no later than 7 years if required for business use.	Records consists of drafts, working/development files and supporting documentation. This excludes significant policy or decision making and drafts with substantive edits or annotations that are to be incorporated into the appropriate Program File. Files include, but not limited to, drafts of correspondence; memoranda; plans; reports; evaluations; assessments; decision papers; position papers; congressional documents; diplomatic notes; testimonies; policies and standards; background notes; press releases issued through the Department's press office or the Diplomatic Security (DS) web site; press guidance for use by the Department's spokesman and DS personnel when speaking to the news media or public audiences; speeches made by the DS Assistant Secretary and Deputy Assistant Secretary; clearances on writing for publication and public speeches given by DS employees on matters of official concern; written responses to media queries; media interviews; information related to media policy guidance; background information on preparation of informational and educational materials; information on outreach programs, such as the A-OK Program (Alert Overseas Kids) and the Sentry Kids Identification System; presentations on DS mission-related topics that are used to support internal and external program activities; information created by DS or created by

• **DS/PA** • **DS/SI** • **DS/T** • **DS/TIA**		and for others on DS mission-related topics, such as copies of news clips and commercial productions or DS internal training topics that are used to support internal and external program activities; and materials for exhibits.

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) On what other entities above is PII maintained in the system?

☐ Members of the Public

☐ U.S. Government employees/Contractor employees

☐ Other

☒ N/A

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

☒Yes ☐No ☐N/A

- If yes, under what authorization?

- Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 U.S.C. § 4802, as amended;
- Social Security Act of 1935
  Foreign Assistance Act, 22 U.S.C. § 2349aa et. seq

(d) How is the PII collected?

Original collectors of PII initiate the process of creating a task by gathering PII from various documents (i.e., passports) and provide it to the TASKR-U end-user. Then, end users manually input the PII into TASKR-U.

(e) 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.

(f) What process is used to determine if the PII is accurate?

There is no process within TASKR-U to validate if the PII entered by the end-user into the system is accurate. It is the responsibility of the original collector of the information to validate the accuracy of the PII they collect prior to submission to the TASKR-U end-user.

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

The original collector of the information is responsible for ensuring currency of the PII at the time it is collected. Once the information is entered into TASKR-U, however, there is no process by which to ensure the PII remains current.

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

No, the system does not use information from commercial sources nor is it publicly available.

(i) How was the minimization of PII in the system considered?

The tasks within the TASKR-U application only include PII that is directly relevant and necessary to accomplish the specified functions of the task. When a task requires PII, users are required to mark the task as PII, which puts a visually striking banner across the page containing documents with PII. This indicator flags the sensitive information for the user so it can be handled appropriately. All tasks within the TASKR-U application are restricted to users with a need-to-know.

5. Use of information

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

The intended use of the PII is to complete a specific task. For example, PII would be included to support validating an individual’s identity. This task would need to include the full name and full SSN to confirm their identity in order to respond to their inquiry.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the use of PII in TASKR-U is relevant to the purpose for which the application is designed because PII is used to facilitate task completion.

TASKR-U is utilized by many different directorates within DS to include Legislative Affairs, which uses the application to respond to Congressional inquiries on behalf of constituents. This is done by creating a task in TASKR-U and attaching a privacy waiver document containing the constituents PII (SSN, DOB, full name etc.) All PII is marked accordingly in the task with a banner.

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

If yes:

(1) What types of methods are used to analyze the PII?
N/A

(2) Does the analysis result in new information?
N/A

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

(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

(d) If the system will use test data, will it include real PII?

☐Yes ☒No ☐N/A

If yes, please provide additional details.

N/A

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal:
No PII will be shared internally.

External:
No PII will be shared externally.

(b) What information will be shared?

Internal:
No PII will be shared internally.

External:
No PII will be shared externally.

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

Internal:
No PII will be shared internally.

External:
No PII will be shared externally.

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

Internal:
No PII will be shared internally.

External:
No PII will be shared externally.

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

Internal:
No PII will be shared internally.

External:
No PII will be shared externally.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Notice is not provided to the record subject. If a task has PII, it is the responsibility of the original collector of the PII to notify the record subject.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☐Yes ☒No

If yes, how do record subjects grant consent?

N/A

If no, why are record subjects not allowed to provide consent?

Any consent responsibilities are the duty of the original collector. The TASKR-U system does not engage directly with record subjects.

(c) What procedures allow record subjects to gain access to their information?

There is no procedure in place to allow record subjects to review their PII within TASKR-U.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☐Yes ☒No

If yes, explain the procedures.

N/A

If no, explain why not.

No, records subject cannot correct inaccurate information within TASKER-U. Record subjects have to reach out to the entity or person (original collector) that made the initial request for PII.

(e) By what means are record subjects notified of the procedures to correct their information?

Record subjects are not notified of procedures to correct their information by TASKR-U end-users. Communication of any procedures to correct information is the responsibility of the original collector

8. Security Controls

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

The TASKR-U application uses Transparent Data Encryption (TDE) on an SQL server database for data at rest. TASKR-U also uses role-based access controls for all end-users. Access to the TASKR-U is based on an end-user's role within the organization and their need-to-know. TASKR-U restricts access to only end-users who are approved by DSS management.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

DS TASKR-U Application Roles	PII Access
General Tasker Group Users (End Users)	Read/write privileges to all PII (in 3d) in any assigned Tasker entries.

Primary/Secondary Tasker Group Owners (End Users)	Read/write privileges to all PII (in 3d) in any assigned Tasker entries
Software Programmers/Developers	Read/write privileges to all PII (in 3d)
Database Administrators	Read/write privileges to all PII (in 3d)

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

For access to the TASKR-U application, management approval is required, and approval is based on a person's role/position, as well as a need-to-know.

End-users are assigned to different groups in TASKR-U based on what information and topics they need to access. End-users with permissions in verified groups will be able to read, write and edit taskers assigned to their groups. End-users' access to a group is verified every 30 days. This ensures that data access is limited to only those with a need-to-know.

TASKR-U also invokes the Department's policy to remove an end-users OpenNet access on his/her last day of service. At that time, it is the responsibility of the end-user's ISSO and/or Manager to process off-boarding paperwork and collect their PIV card. ISSOs and/or Managers are responsible for submitting tickets to disable or delete an end-users OpenNet account and share the information with respective TASKR-U primary/secondary tasker group owners.

(d) How is access to data in the system determined for each role identified above?

All user roles listed above submit an AccessDS request to a specified group. The request is routed to the primary/secondary group owners and product owners via email to grant permissions. Upon approval, the end-user is notified of the status of his/her access request via e-mail.

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

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

The TASKR-U application uses Splunk to monitor and display information provided by application logging. Application logging provides information on end-user interactions with the application, such as when Application Programming Interface (API) endpoints are invoked, web requests are initiated, session information, and capturing end-user login credentials. Primary/Secondary Tasker group owners also receive an email every 60 days to validate end-users in their Tasker group. Primary/secondary Tasker group owners can manually remove/add end-users.

TASKR-U also has custom email workflows to conduct daily automated audits of the TASKR-U end-user list to flag inactive users. When a user's profile is marked as inactive (no activity within the last 60 days), they are automatically removed from TASKR-U and must request access again through AccessDS.

TASKR-U also invokes Department of State policy to remove an end-users OpenNet access on his/her last day of service. At that time, it is the responsibility of the end-user's ISSO and/or Manager to process off-boarding paperwork and collect their PIV card. ISSOs and/or Managers are responsible for submitting tickets to disable or delete an end-users OpenNet account and share the information with respective TASKR-U primary/secondary tasker group owners.

(d) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(e) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

Users are required to complete the annual cybersecurity training PS800: Cybersecurity Awareness which includes a module on privacy. Additionally, all users are required to take the biennial training PA318: Protecting Personally Identifiable Information.