

PRIVACY IMPACT ASSESSMENT

Cascades

1. Contact Information

A/GIS Deputy Assistant Secretary

Bureau of Administration
Global Information Services

2. System Information

- (a) **Date of completion of this PIA:** February 2022
- (b) **Name of system:** Cascades
- (c) **System acronym:** N/A
- (d) **Bureau:** Bureau of the Secretary (S/ES-ExecTech)
- (e) **iMatrix Asset ID Number:** 318964
- (f) **Child systems (if applicable) and iMatrix Asset ID Number:** 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:**

Cascades is an integrated platform for tasking, tracking, drafting, clearing, reviewing, and archiving all Executive Secretariat (S/ES) paper processed by the Executive Secretariat Staff (S/ES-S) (i.e., the “Line”). Features include a shared collaborative workspace for both S/ES and bureau users; flexible workflows; auto-generated templates; ability to integrate data visualization tools; sophisticated metrics and diagnostics; and a searchable,

comprehensive document library. The OpenNet version is a custom written application residing in Azure, with the data stored in SharePoint Online (Office365).

Cascades maintains information used in preparation for meetings including biographical information of members of the public, U.S. Government employees/contractor employees, and non-U.S. persons engaging with the Department. Only the biographies portion of Cascades processes searches or displays personally identifiable information (PII). *The remainder of this PIA will only focus on the PII collected through the biographies.*

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

The system collects and uses the following information: Name, job title, and photograph.

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

22 U.S.C. 2651a – Organization of the Department of State

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

Yes, provide:

- SORN Name and Number:
Secretariat Contact Records, STATE-84

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
August 24, 2020

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)):
A-27-003-04a and A-27-003-04b
- Disposition Authority Number:
DAA-0059-2014-0015-0001 and DAA-0059-2014-0015-0002
- Length of time the information is retained in the system:
The information in Cascades is considered permanent and will be kept by the Department for 25 years and eventually turned over to the National Archives and Records Administration for the life of the republic.
- Type of information retained in the system:
Cascades is a powerful collaboration tool for facilitating the flow of information to and from the Secretary of State and other senior Department principals; Cascades provides the ability to receive foreign policy memoranda and correspondence from Department bureaus and offices electronically, as well as task and track the paperless submission of most memoranda. Correspondence and memoranda can include internal and external letters, action memos, information memos, briefing checklists, and telephone talking points, as well as documents received from other agencies.

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?

(d) How is the PII collected?

There is one designated person in each bureau (analyst or desk officer) that inputs information into the system based on known facts, previous meetings, and/or information obtained directly through public web search engines.

(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.

Cascades is a cross domain system with some data stored in SharePoint online. All information inherits the controls and safeguards implemented to Office365.

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

The information collected for biographies is publicly available and deemed trusted and verified through research before the information is internally shared. Once received in Cascades, the information is passed through a clearance process per 2 FAM 1200 Action and Clearance Procedures. In addition, S/ES is considered the tasking office and is responsible for coordination of the work for the Department internally. S/ES utilizes templates to ensure details are accurately outlined in submissions. Information is deemed appropriate at the time of entry and there is no expectation of accuracy after date entered.

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

The information is deemed current at time of entry. No further steps are taken to update the information once it's received.

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

No, the system does not use information from commercial sources. Information is collected from public sources but is not made public by the Department once entered into the system.

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

Only the minimum amount of PII necessary to meet operational goals is collected. For instance, during the system development requirements phase, it was determined that SSNs are not needed for operation of the system and so SSNs are not collected.

5. Use of information

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

The information collected is used to inform a principal on the individuals they are scheduled to meet.

(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, Cascades has several business functions to include the use of biographies that are being used at all levels in the Department of State. Biographies are used for Trip Books, preparations for inter-agency meetings, and pre-planning. Cascades also serve as an integrated platform for tasking, tracking, drafting, clearing, reviewing and archiving all S/ES paper processed by S/ES-S. However, those processes generally do not contain PII.

(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?

(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

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

Yes No N/A

If yes, please provide additional details.

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

Internal: Cascades does not share information internally.

External: Cascades does not share information externally.

(b) What information will be shared?

Internal: N/A

External: N/A

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

Internal: N/A

External: N/A

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

Internal: N/A

External: N/A

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

Internal: N/A

External: N/A

7. Redress and Notification

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

Information is not collected directly from the individual thus notice prior to the collection is not given.

(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?

If no, why are record subjects not allowed to provide consent?
The PII is not collected from the record subject directly.

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

Though record subjects are not provided access to the Cascades system, the Department's Privacy Act practices allow for record subjects to gain access to their information by contacting the Department's Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the covering SORN State-84, Secretariat Contact Records.

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

Yes No

If yes, explain the procedures.

The Department's Privacy Act practices allow for record subjects to gain access to and correct their information by contacting the Department's Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the covering SORN State-84, Secretariat Contact Records.

If no, explain why not.

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

Since information is not collected directly from record subjects, they are not notified of the procedures to correct their information. Department's Privacy Act practices allow for record subjects to correct their information by contacting the Department's Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the covering SORN State-84, Secretariat Contact Records.

8. Security Controls

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

The information in Cascades is secured by security controls, safeguards, and authentication security measures. Cascades is initially managed through Microsoft's Active Directory Services and controlled by use of logical access controls. Logical access control refers to specific privileges set that grant users a certain level of access to the information based on role, job duty, and need-to-know. Additionally, NIST SP-800-53 security controls are implemented to protect the information within the system. The Department utilizes Multifactor Authentication (MFA) and Personal Identity Verification as an added layer to single sign-on which further protects the data within the information system. The information is being protected through FIPS 140-2 encryption algorithm through Microsoft Office 365.

(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).

The following roles have access to name, job title, and business photograph:

System administrators: Are responsible for system maintenance including installing, upgrading, and monitoring software and hardware, as well as maintaining the essentials

such as operating systems and business applications. The system administrators also monitor the information system, review security logs on the monthly basis, and approve access to the system.

General users: Program management officers, desk officers and subject matter experts engaged in content creation, tasking response, data tracking and monitoring.

Line users: S/ES-S and ExecSec Front Office staff engaged in content creation, tasking delegation, data tracking and monitoring.

Front office users: All functional and regional bureaus within the Department that inform senior principal officers. Front office users act as final approvers and consumers of the finalized product.

(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.

System access is initiated by a front office user. Access to Cascades is granted by leadership personnel (Front Office staff and system administrators). Once access has been granted, access is controlled through Active Directory in accordance with Access Management policies and in compliance with the Department’s privacy rules of behavior for protecting PII. Access controls have also been implemented to enforce user access within Active Directory with least privilege access.

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

A manual request to access the system is initiated by a front office user. Access for all users undergo the same process which includes a signed user agreement confirming adherence to all Department IT and data privacy regulations. Determining each role’s access to PII is based on the principle of least privilege and the job requirements of that role. Access to Cascades is granted by leadership personnel (Front Office staff and system administrators). Once access has been granted, access is controlled through Active Directory.

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

The system administrators can run auditing reports (not available to general users) for system maintenance and accountability purposes. Splunk and LogRhythm are utilized to monitor and capture audit logs.

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

Yes No

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

There is no specific role-based training. All authorized users of Cascades sign an agreement attesting they will abide by Department IT policies, including those involving data privacy. All users are trained on policies regarding sharing of information during functional training and in-processing. All authorized Department users identified in 8(b) must complete the mandatory annual security training PS800: Cyber Security Awareness, which has a privacy component, and the biennial privacy training PA318: Protecting Personally Identifiable Information.