

PRIVACY IMPACT ASSESSMENT

SYNCH 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:** 12/2022

(b) **Name of system:** System Namecheck

(c) **System acronym:** SYNCH

(d) **Bureau:** Diplomatic Security (DS)

(e) **iMatrix Asset ID Number:** 487

(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:**

SYNCH automates the tasks associated with tracking DS personnel (employees and contractors) clearance status and clearance folder locations. The application maintains information on clearance type, status, case open and close dates, clearance dates, investigation type, case code and number, and folder location. SYNCH satisfies the

Personnel Security and Suitability Division (DS/SI/PSS) requirement to track clearance information in a classified environment.

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

- Full Name (First, Middle, Last name)
- Social Security Number (full and/or partial)
- Date of Birth
- Place of Birth

(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, as amended, 22 U.S.C. § 4801 et seq.;
- Executive Order 12968, as amended (Access to Classified Information);
- Executive Order 13467, as amended (Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information);
- EO 9397 Numbering System for Federal Accounts Relating to Individual Persons;
- 28 CFR § 16.53 - Use and collection of social security numbers

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

☒ 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 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: Personnel Security and Access Clearance Records, DAA-GRS-2017-0006-0024

-Disposition Authority Number: GRS 5.6, item 180

-Length of time the information is retained in the system: Temporary. Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use.

-Type of information retained in the system: Records of people not issued clearances. Includes case files of applicants not hired.

Records about security clearances, and other clearances for access to Government facilities or to sensitive data, created to support initial favorable eligibility determinations, periodic reinvestigations, or to implement a continuous evaluation program. Includes:

- questionnaires
- summaries of reports prepared by the investigating agency
- documentation of agency adjudication process and final determination

Schedule number: Index to the Personnel Security Case Files, DAA-GRS-2017-0006-0026

-Disposition Authority Number: GRS 5.6, item 190

-Length of time the information is retained in the system: Temporary. Destroy when superseded or obsolete.

-Type of information retained in the system: Lists or reports showing the current security clearance status of individuals.

Schedule number: Personnel Security and Access Clearance Records, DAA-GRS-2017-0006-0025

-Disposition Authority Number: GRS 5.6, item 181

-Length of time the information is retained in the system: Temporary. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use. (Supersedes GRS 18, item 22a)

-Type of information retained in the system: Records of people issued clearances. Records about security clearances, and other clearances for access to Government facilities or to sensitive data, created to support initial favorable eligibility determinations, periodic reinvestigations, or to implement a continuous evaluation program. Includes:

- questionnaires
- summaries of reports prepared by the investigating agency
- documentation of agency adjudication process and final determination

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, as amended, 22 U.S.C. § 4801 et seq.;
- [Executive Order 12968](#), as amended (Access to Classified Information);
- [Executive Order 13467](#), as amended (Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information);
- Executive Order 9397 Numbering System for Federal Accounts Relating to Individual Persons;
- 28 CFR § 16.53, Use and collection of social security numbers

(d) How is the PII collected?

Information is primarily obtained from other Department offices via e-mail and, on rare occasions, by phone/verbal communication.

(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.
N/A

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

Information for SYNCH is obtained from other Department offices. The data is vetted through the originating data collection points from the other organizations via their processes prior to being input into SYNCH.

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

Clearance information is reviewed as needed based on investigations.

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

No commercial sources are used, and the information is not publicly available.

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

SYNCH only uses the necessary PII to check on the clearance statues on persons identified in 4a. Unnecessary PII is not collected due to the inherent security risk of gathering and managing PII that is not needed to fulfill the mission requirements.

5. Use of information

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

The information in SYNCH helps facilitate tasks associated with tracking DS personnel (employees and contractors) clearance status and clearance folder locations. The information stored in SYNCH facilitates security clearance determination related to national security and supporting the DS mission. SYNCH's business process facilitates the administrative and operational case information of new hires and certain contractors related to government clearances.

(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 PII collected as notated in Section 3d is relevant for use with SYNCH to help distinguish individuals' security clearance statuses.

(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:

There is no internal sharing.

External:

There is no external sharing.

(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?**

SYNCH is not the original collector of the information. SYNCH receives information from other sources, and it is the source system's responsibility to ensure notice is provided to the record subject when the information is originally collected.

(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?

SYNCH is not the original collector of the information. SYNCH receives information from other sources. If an individual declines to provide the PII to the original collector of the information, the process is unable to proceed.

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

SYNCH is not the original collector of the information. SYNCH receives information from other sources. No procedures exist for record subjects to gain access to their information in SYNCH.

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

☐ Yes ☒ No

If yes, explain the procedures.

If no, explain why not.

SYNCH is not the original collector of the information. SYNCH receives information from other sources. SYNCH receives its data in read-only format and any correction of record subject information must be accomplished at the source system.

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

There is no notification process for individuals to correct their information. SYNCH is not the original collector of the information. SYNCH receives information from other sources.

8. Security Controls

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

SYNCH has the appropriate management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act of 2002, and the information assurance standards published by NIST Special Publications 800-Series (NSIT SP 800-84).

(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).

SYNCH Users - Users are responsible for collecting and processing all PII in SYNCH to track background investigation and adjudication information for the Department. The users can create, read, update, and search data in the system.

SYNCH View Only - They have restricted roles and use SYNCH to review personnel security actions to support their office's mission. They have read-only access to all PII and cannot create or update information.

SYNCH Admin - System administrators establish system accounts, configuring access authorizations (i.e., permissions, privileges), troubleshoot and triage system issues. Administrators don't have access to PII.

(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.

Management approves user access to SYNCH based on role and need-to-know.

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

SYNCH Users, SYNCH View Only users, and SYNCH Admins request access via the AccessDS application. Supervisor, Business Owner, and Information System Security Officer (ISSO) are included in the approval chain for all accounts.

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

SYNCH leverages the controls in place native to ClassNet. Monthly auditing exists within the SYNCH application and data transactions are tracked automatically in the database and User Interface.

(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.

Users are required to be in compliance with mandatory security (PS800 Cyber Security Awareness) and privacy (PA318 Protecting Personally Identifiable Information) training required for all authorized users to ensure they understand the proper protocols for protecting the vast amounts of PII they have access to. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. The Protecting Personally Identifiable Information training is a biennial requirement.