Privacy Impact Assessment
of the
ServiceNow HR Service Delivery HRSD System (HRSD)

System Owner:

Board of Governors of the Federal Reserve System's (Board) Division of Management

Contact information:

System Manager:	Lewis Andrews
Title:	Assistant Director, HR
Division:	Division of Management
Address:	20th Street and Constitution Avenue, N.W. Washington, DC 20551
Telephone:	(202) 452-3082

IT System Manager:	Nikole Fernandez-Rivera
Title:	Manager, Systems & Compliance
Division:	Division of Management
Address:	20th Street and Constitution Avenue, N.W. Washington, DC 20551
Telephone:	(202) 973-7336

Description of the system:

The ServiceNow HR Service Delivery (HRSD) System is a customer relationship management (CRM) module within the cloud-based ServiceNow platform that focuses on employee relations and case management, as well as providing an employee service center portal solution for active employee self-service. This system manages human resource (HR) and payroll inquiries related to current and former Board employees. The system provides the following functions: knowledge bases for active employee self-service, integration to Computer Telephony

Integration (CTI)[1], case management[2], workflows with approvals, Service Level Agreements (SLAs) management, notifications, reporting, and form/document management.

1. The information concerning individuals that is being collected and/or maintained:

The population within this system includes current and former Board employees and members of the public, including recruits, applicants, and hires.

For current and former Board employees, ServiceNow HRSD collects the following information for two types of profiles: the User Profile and the HR Profile. The User Profile is required for any user to access the ServiceNow platform and is populated from the Board's identity and access system. In the event an employee became inactive prior to September 2020, an "inactive" User Profile has been created by the HR Profile creation process. The HR Profile is populated from the Board's personnel system and is used to populate basic personal information about an employee. Active and inactive Board employees have User Profiles and HR Profiles in HRSD.

User Profile

- First and last name;
- Division;
- Work email address;
- Name of manager; and
- Title.

HR Profile

- Legal first name and middle name;
- Date of birth;
- Social Security number;
- Employment information (employee number, start and end dates, and employment type);
- Home address;
- Leave status;
- Marital status;
- Personal contact information (personal email and mobile number);
- Work contact information (work phone and mobile phone[3]);
- Active or inactive status;
- Gender;
- Salary;

[1] This Privacy Impact Assessment also covers the CTI itself.
[2] The term "case" is used to identify a ticket or workflow process in HRSD.
[3] Not all individuals in this system are assigned a mobile number.

- Officer flag;
- Manager flag;
- Salary grade; and
- Race/Ethnicity.

For current Board employees who are filing a Full-Time Temporary Telework Request, the following information is solicited:

- Subject Person (Name);
- Division Director (Name);
- Business Management Analyst (Name);
- Agreement Type; and
- Reason for Request (including supporting documentation).

The Reason for Request field is a free-form completion where a Board employee submits the reason they should be considered for Full-Time Temporary Telework as well as documentation in support of the request. Such reasons may include a request to telework in lieu of using the Family and Medical Leave Act (FMLA), paid parental leave, sick leave, or short-term disability. Other circumstances for such a request could be a request for telework when an employee experiences a hardship, such as a natural disaster, a family member has a serious medical condition, or other personal hardships, such as a divorce or spousal abuse.

Former employees or members of the public (spouses, survivors, dependents, etc.) who need support get in contact via phone. If a former employee is not found in this system, identity verification is carried out by reviewing the Board's personnel system outside of HRSD. In this instance, a generic case can be opened with only the minimal PII to obtain service. Current employees may also receive support via phone. The CTI collects and uses one or more types of the following information when accessing the system via telephone:

- Phone number;
- Employee ID;
- Case number (optional and originally generated by HRSD); and
- CTI-generated call reference number.

For those recruits, applicants, and/or hires who engage in a pre-employment action (travel or education verification), one or more of the following information types is collected by this system:

- Name;
- Date of birth;
- Social Security number;

- Hiring division;
- Education Information (school, location, degree level, major, and degree year);
- Taleo job number;
- Home address (street address, city, state/province, zip code, and country);
- Phone number;
- Email address;
- Redress number (as needed);
- Gender;
- Interview information (date and time); and
- Booking information (travel details, including mode, airport/rail code, hotel, departure and arrival cities, and purpose);

As needed to effectively document facts pertinent to a case, information regarding other individuals may appear in this system via several free-form fields or as attached documents to the case. Moreover, information regarding certain pre-employment actions may appear in this system for recruits, applicants and/or hires.[4]

HRSD is the Board's primary system for tracking support requests for HR functions. Reports generated in the Board's human resources, onboarding, or recruiting systems are attached to a ticket in HRSD as part of a reporting workflow. These reports can contain any information from the Board's human resources, onboarding, or recruiting systems.

2. Source(s) of each category of information listed in item 1:

For current and former employees, the initial source for the HR Profile is the employee themselves during the recruiting and onboarding phases where such information is entered into the Board's human resources system, which is then used to populate the HR Profile in HRSD. The Board's identity and access system obtains the initial information for the User Profile from the Board's human resources system for all employees as of September 2020. For former employees prior to September 2020, a User Profile is created by the HR Profile integration from the Board's human resources system. HRSD then obtains the User Profile information from the Board's identity and access system. The current employee supplies any necessary additional information to resolve a case.

Information related to the Employee Relations (ER) module may be provided by an employee or former employee themselves or may be solicited by a Board employee from an individual during the course of an issue resolution.

[4] Recruits and applicants are individuals who have applied for employment at the Board but who have not received an offer while hires are individuals who have applied for employment and accepted an offer from the Board but have not yet entered employee status.

Information related to the telephone integration system is provided by the caller except for system-generated call reference number.

Information related to the pre-employment actions is provided by the candidate, recruit, or hire.

3. Purposes for which the information is being collected:

HRSD automates certain HR interactions and provides a single platform for all HR services to originate. The information that is collected upon creating a case within HRSD ensures that HR service requests can be properly resolved.

The information contained in the HR Profiles and User Profiles is utilized to support verification that a person calling into the HR helpdesk is a current or former Board employee[5], to enable an automated workflow, to assist in the completion of forms created as part of the delivery of an HR service, to send notifications, and to restrict access to certain types of services and knowledge base content.

The information collected within ER cases ensures relevant information is available, so that involved parties, allegations/issues, investigation notes, corrective actions, and resolutions are properly documented. The information also is utilized in ER reporting.

The information collected within a general helpdesk case is utilized to describe the request and to document the resolution that was provided to the employee or former employee.

The information collected by the CTI is used to direct callers to the appropriate resource.

The information collected during the pre-employment action is used to facilitate travel arrangements for recruits or applicants and for verification of education for hires.

4. Who will have access to the information:

Access to the information maintained in ServiceNow HRSD is limited to authorized users, which consists of Board employees who access the information on a need-to-know basis. Access to the information is restricted to that which is required in the performance of the user's duties. This information may also be disclosed for the purposes set forth in the Systems of Records entitled BGFRS-6 "Disciplinary and Adverse Action Records" and BGFRS-26 "Employee Relations Records."

5. Whether the individuals to whom the information pertains have an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses):

[5] This verification step uses Employee ID, last 4 digits of SNN and Phone Number to assist the HR helpdesk.

Individuals do not have the ability to consent to uses of their information contained in the system. With regards to data in a specific case, individuals may decline to provide information but doing so may impact obtaining information related to their case, inquiry, or request.

6. Procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date:

An individual may request changes in the source human resources system or access and identity system if the information is out of date, incorrect, or incomplete. HRSD does not have the ability to make direct changes in those systems.

The data captured in the administration of a case is the responsibility of the Board employee working the case and cannot be accessed by the person who opened the case. Should the Board become aware of a discrepancy in the information within this system, corrective action will be taken to update that information.

7. The length of time the data will be retained and how will it be purged:

The official retention period for records in connection with ER cases is 7 years after closure. For help desk-related records it is one year after case closure. The Board is currently reviewing data purging options within the ServiceNow platform for case data. Until a solution is developed, the data will be retained indefinitely.

8. The administrative and technological procedures used to secure the information against unauthorized access:

ServiceNow HRSD tracks individual user actions within the system. The audit and accountability controls are based on NIST and Board standards which, in turn, are based on applicable laws and regulations, including the Federal Risk and Authorization Management Program (FedRAMP). The controls assist in detecting security violations and misuse of information in the ServiceNow HRSD system. The Board is solely responsible for a subset of the total controls for this system, has joint responsibility for another subset of controls with the Cloud Service Provider (CSP), and the CSP is solely responsible for the final subset of controls.

Access to ServiceNow HRSD is restricted to authorized Board employees who require access for official business purposes. See Section 4 of this Assessment for additional details.

Users are classified into different roles and access and usage rights are established for each role. User roles are used to delineate between the different types of access requirements so users are restricted to only accessing PII data that is required in the performance of their duties.

Periodic audits and reviews are conducted to determine whether individual users still require access, have the appropriate role, and whether there have been any unauthorized changes to information maintained in the ServiceNow HRSD system. This system undergoes an annual review under the Federal Information Security Modernization Act (FISMA).

9. Whether a new system of records under the Privacy Act will be created. (If the data are retrieved by name, unique number or other identifier assigned to an individual, then a Privacy Act system of records may be created):

The ServiceNow HRSD system is covered by two Systems of Records entitled BGFRS-6, "FRB—Disciplinary and Adverse Action Records" and BGFRS-26, "FRB—Employee Relations Records." Information governed by the following Systems of Records is utilized on a read-only basis by ServiceNow HRSD: BGFRS-1, "FRB—Recruiting, Placement and Onboarding Records" and BGFRS-4, "FRB—General Personnel Records." Records related to exceptions to the Board's Academic Assistance Policy are governed by BGFRS-30, "FRB—Academic Assistance Program Files."

Reviewed:

/signed/ ***12/14/2022***

Andrew Krug — Date
Senior Agency Official for Privacy

/signed/ ***12/14/2022***

Kofi Sapong — Date
Chief Information Officer (Interim)