Privacy Impact Assessment for

Executive and Schedule C System (ESCS)

September 2025

Contact Point
Edward Smith
System Owner
Lead Business Systems Specialist
Executive Service and Workforce Development
Workforce Policy and Innovation

Reviewing Official
Becky Ronayne
Acting Senior Agency Official for Privacy

Abstract

The Office of Personnel Management's Executive and Schedule C System (ESCS) is administered by the Policy and Special Programs group within the Executive Services and Workforce Development Center of the Workforce Policy and Innovation office. ESCS stores information on career and non-career (*i.e.*, civil service and politically appointed) executives and appointees. This PIA is being conducted because information about those executives and appointees is used, collected, maintained, and disseminated in ESCS.

Overview

The Office of Personnel Management's Executive and Schedule C System (ESCS) is administered by the Policy and Special Programs group within the Executive Services and Workforce Development Center of the Workforce Policy and Innovation office. ESCS is a web-based human resources application that collects and maintains information needed to manage certain executives and appointees and assure they are hired and appointed in compliance with the regulatory and statutory requirements.

ESCS collects information on the following executives and appointees:

- Senior Executive Services (SESs): SES are the federal government's core of executives that provide leadership and managerial expertise in Executive Branch Agency mission program areas. These individuals may be politically appointed (non-career) or hired through a non-political process (temporary or career).
- Senior Leaders (SLs): The SL category was established in 1990 to replace GS-16, 17, and 18 positions. Most SL employees hold positions with duties broad and complex enough to be classified above a GS-15. Agencies that are statutorily exempt from having Senior Executive Service (SES) staff fill their executive positions with SL staff. These individuals are hired through a non-political process.
- Science and Professional employees (STs): ST employees engage in work that involves high-level research and development in the physical, biological, medical, or engineering sciences, or a closely-related field. These individuals are hired through a non-political process.

- Schedule C appointees: A Schedule C appointment is a political appointment to serve in a confidential or policy role under another appointee. Most Schedule C employees are confidential assistants, policy experts, special counsel, and schedulers, though some serve in specialized non-policy support roles.
- Presidential appointments with or without senate confirmation (PA/PAS appointments): These individuals are either appointed by the president or recommended by the president and confirmed by the Senate.

ESCS also collects information on individuals who have graduated from an OPM-approved agency SES candidate development program (CDP) and are now eligible to become an SES.

A few registered users in each Federal agency, usually HR Specialists or White House Liaisons, can access ESCS. They use the system to view and add information and documents about the executives and appointees in their agency and ask for new staff or to transfer existing staff. These agency staff can also use a business intelligence tool in ESCS called WebFocus to run reports on their staff, positions, and incumbencies.

A few registered users in OPM's Executive Service and Workforce Development office (ESWD) can access ESCS. They use ESCS to help agency staff when they need system assistance or do not have access to ESCS. They assure agency requests for new political staff are approved by the White House Presidential Personnel Office and career staff have been approved by a Qualifications Review Board (QRB) before they are appointed. They assure the government is complying with various requirements, like assuring an agency does not appoint more political staff than permitted. ESCS staff also use ESCS to generate data which goes into the United States Government Policy and Supporting Positions (Plum Book) and PLUM Reporting Portal required by the PLUM Act of 2022, which are used by the White House, agencies across the government, and the media.

All ESCS users must formally request access to ESCS. They must sign a user agreement and only receive access to the information relevant to their respective agency and their role within the agency or other related agencies when given permission to view that data. Reports are run monthly to identify users that have been inactive for a period of time. These accounts are then

reviewed, and if appropriate, deactivated. These processes and security features have been implemented to help protect the privacy of the individuals whose information is collected and stored in ESCS and to help mitigate any possible security risks.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

General authority for the establishment and management of SES, SL, and ST positions can be found in 5 U.S.C. § 3104, 3133-3134, 3324-3325, 3391-3397, 3591-3596, 4311-4315, 5108, and 5381-5385. Specific reporting requirements are authorized by 5 C.F.R. § 9.2, Reporting Workforce Information, and 5 C.F.R. § 214.203, Reporting Requirements.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

ESCS is covered by the OPM Central–13, Executive Personnel Records SORN.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes. A system security plan has been completed for ESCS in conjunction with its Authority to Operate (ATO).

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The information contained in ESCS is subject to NARA-approved schedule N1-478-95-003. The retention for this schedule is to destroy when no longer needed for administrative purposes.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

During the initial application and hiring process, PRA forms such as one's USAJOBS Profile (3206-0219) or Optional Form 306, *Declaration for Federal*

Employment, (3206-0182) may be collected. Otherwise, ESCS relies on data provided by agencies, instrumentalities, or employees of the United States in their official capacities, which is are generally not subject to the PRA per 44 U.S.C. § 4502(3)(A), unless those collections are for "general statistical purposes."

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

For individuals who are appointed or hired to agency positions, ESCS collects, uses, disseminates, and maintains demographic, appointment, and assignment information (*e.g.*, name, office address, date of birth, Social Security number, sex, race and ethnic designation, titles of positions, pay rate, types of appointments) and background data on work experience, educational experience, publications or awards, including performance ratings and any performance, rank, or incentive awards received, and career interests. ESCS collects, uses, and maintains determinations on nominees for Meritorious and Distinguished Presidential Rank awards (but not the investigation information), determinations concerning executive qualifications and the information relating to current and former participants in the sabbatical leave program (including dates of participation and reasons for the leave).

ESCS contains additional information on SESs such as whether they were recruited from another Federal agency or from outside the Federal service and why those who are seeking reemployment as an SES previously left the position (e.g., retired, resigned, to enter private industry, to work for a state government, or removed during probation or after because of performance).

If someone goes through the SES candidate development program (CDP) but has yet been appointed, ESCS collects their name, email, demographic information, the training they were in, and their contact information.

If someone receives access to ESCS, the system collects their name, email address, agency, and work phone number.

2.2. What are the sources of the information and how is the information collected for the project?

The information about the staff at an agency is generally entered by the HR staff within their agency. Some agencies do not assign staff to access ESCS, so OPM ESWD staff upload the data as requested by that agency. A lot of the information on career staff originally comes from the system used to hire the individual (*e.g.*, USAJobs) while the information on political staff often comes from the White House.

Agency staff can request but not approve an executive's appointment or make certain other changes so that information comes from other sources. The White House Presidential Personnel Office is responsible for approving political appointments, but they do not have access to ESCS, so the OPM White House Liaison, Executive Assistant within OPM's Office of the Director, or OPM ESWD staff add the approval to ESCS on their behalf. Certain staffing changes, such as moving from a political to career role, can only be approved by OPM ESWD staff.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

ESCS does not use any information from commercial sources or publicly available information.

2.4. Discuss how accuracy of the data is ensured.

In most situations, Agency HR Specialists and White House Liaisons, who are most familiar with the individuals in their agency, enter information about their executives and appointees into ESCS and can then access the system to verify that information. In a few situations, an agency will not assign staff to access ESCS, so OPM ESWD staff add the data as requested. Regardless of how an agency chooses to use the system, OPM ESWD staff send agencies copies of information about their own agency executives and appointees so they can verify accuracy and make updates where necessary. If the agency cannot update the information themselves, they can email OPM ESWD staff to make the change.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the system will collect more information than is necessary to achieve its business purpose.

Mitigation: This risk is mitigated by placing most of the input and correction responsibilities with the authorized agency users. These agency users are in the best position to know and understand what is needed to fulfill the agency's business need.

Privacy Risk: There is a risk that the information in ESCS is not accurate and will result in inaccurate management of the program or adverse performance decisions.

Mitigation: This risk is mitigated by making agency users responsible for validating the information in the system. OPM ESWD staff can work with an agency user to correct the data and verify the updates.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

The information in ESCS is used to manage the appointing of executives and appointees. It is used to make hiring and appointment decisions, comply with relevant statutes and regulations, including the allocation and establishment of positions, development of qualification standards for SES positions, operation of QRBs, establishment of programs to develop candidates for and incumbents of executive positions, and development of the performance appraisal systems. The information may also be used to determine trends, such as from where staff are coming from or why staff may be leaving their positions.

ESCS includes a business intelligence tool called WebFOCUS that allows agency users to run reports on their agency's information. The information in the reports is used for policy formulation, program planning and administration, research studies, and required reporting.

Social Security numbers (SSNs) are used to uniquely identify an individual. The SSN is the only reliable unique identifier to ensure that data is not

duplicated or applied to incorrect individuals. SSNs are initially provided by the individual and entered into the system by agency users.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

ESCS uses SQL queries built into the application to return specific records from the database to display them on the screen, update records in the database, and create new records in the database. No artificial intelligence or other special technologies are used to electronically search, query, or analyze the database to discover or locate a predictive pattern or an anomaly.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

The following staff have access to ESCS:

- OPM ESWD staff can access and change almost all the information in ESCS since they are asked by agencies and leadership to make ESCS changes on their behalf.
- Certain members of OPM OCIO have access to ESCS to manage the technical aspects of the system.
- The OPM White House Liaison and the Executive Assistant within OPM's Office of the Director can access information on political staff so they can approve their appointments in the system.
- Outside of OPM, HR Specialists and White House Liaisons within various federal agencies have access to information about the people within their agency.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that an unauthorized user may access the system, or that an authorized user may access information for an impermissible use.

Mitigation: This risk is mitigated by using access controls that restrict user access to the information they need to know based on authorization and access permissions in the system. For example:

- Individual agency users may only view information about staff in their agency.
- White House Liaisons within an agency may generally access only information about political appointees, while HR specialists within an agency have access to both career and political appointee information.

When users apply for access to ESCS they identify which agencies they are affiliated with and their role at those agencies, and their supervisor must approve the request. The user is also required to sign and comply with ESCS OPM Access Request. This document outlines the proper use of the system based on their roles.

All users are only permitted to access data that are expressly authorized to the user. Audits are completed on user login frequency and user accounts that have not logged in within 60 days are disabled. The user must submit a request to OPM Program Office to have their account re-enabled.

This risk is further mitigated by limiting information within ESCS that can only be provided by the agency user and only permitting retrieval of information via pre-defined reports. In addition, all users are required to adhere to Rules of Behavior that govern the appropriate access and use of the system.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Executives and appointees do not interact directly with the system and therefore do not receive direct notice from ESCS or specifically about ESCS. Much of the information in ESCS is provided by agency staff in the normal course of the human resources lifecycle and appropriate notice about the collection and use of that information is provided at various points. However, executives and appointees could ask their agency staff to explain what

information is in ESCS. In addition, they also receive notice about ESCS through the OPM/CENTRAL-13 SORN and the publication of this PIA.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Applying for executive positions is voluntary but once individuals have provided their information in the human resources process, they are not given an opportunity to opt out of their information being included in ESCS.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that executives and appointees were not provided notice prior to the collection of their information and are unaware that their information is in ESCS.

Mitigation: This risk is mitigated by providing general notice at various points of collection in the human resource process and by agencies providing information to employees concerning the executive service and how their information is used.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

The information captured in ESCS is retained for as long as is necessary for administrative purposes in accordance with the NARA-approved records schedule N1-478-95-003. As stated in N1-478-95-003, Electronic database files containing information on:

A. Present and former incumbents of executive positions, including demographic appointment and assignment information;
B. Executive positions;
C. Actions requiring approval by OPM or other authority, and
D. Federal agencies.

Records must be destroyed when no longer needed for administrative purposes.

Because ESCS tracks an individual's career with the government and because an individual can be reinstated after they leave government service, individual records and information related to their employment history are retained even after they depart the government.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information in ESCS will be retained for longer than is necessary for its intended purpose.

Mitigation: This risk is partially mitigated because there is a records schedule in place. The records schedule calls for the records to be destroyed when no longer needed for administrative purposes and the program office will work with OPM's records officer to determine the appropriate retention period.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Agency users can access and use the information in ESCS about their own agency personnel when they have a need-to-know. For example, agency White House Liaisons are only permitted to access information about their agency's political appointees.

If someone in an agency has access to see records on someone who is an SES or Schedule C appointee, they can see records on all their prior SES or Schedule C positions, even if they were at a different agency. This is limited to read only data of what the title was, and the dates the individual was in that position.

Reports with a government-wide scope can be generated by the system and provided to the White House. The information shared outside of OPM is used for policy formulation, program planning and administration, research studies, and required reports regarding the Government-wide executive program.

Except for OPM White House Liaisons and designated ESWD and OPM Employee Services personnel, all participating agency users have access only to their own agency-specific data through pre-defined reports.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The external sharing described above is compatible with the purpose for which the information was collected, which is to assist OPM in carrying out its responsibilities related to career and non-career SES positions and Schedule C appointments. The OPM/CENTRAL-13 SORN contains appropriate routine uses that are compatible with this purpose and permit the sharing described. Routine Uses a, c and f are relevant:

> *a. To identify and refer qualified current or former Federal employees to Federal agencies for executive vacancies.*
>
> *c. To provide an employing agency with extracts from the records of that agency's employees in the system.*
>
> *f. To provide information to the White House on executives with non-career appointments in the Senior Executive Service, in positions formerly in the General Schedule filled by non-career executive assignments, in excepted positions paid at Executive Schedule pay rates, and in positions in the Senior Level pay system or other pay systems equivalent to those described which are filled by Presidential appointment or excepted from the competitive service because they are of a confidential or policy-determining character.*

6.3. Does the project place limitations on re-dissemination?

As with most disclosures under the Privacy Act, there generally are no specific limitations on re-dissemination placed on the entities to whom OPM provides information from ESCS. However, all users must sign the ESCS Access Request form which details the appropriate access and use of the sensitive information contained in ESCS.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

ESCS creates audit logs that capture when users access the system, what information they saw, and any changes they made to a record.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information in ESCS that is shared with external entities may be used for a purpose other than that for which it was originally collected.

Mitigation: This risk is mitigated using role-based access controls that permit agency users to obtain only information about their own agency when they access the system. In addition, when the OPM Program Office creates and runs reports containing information cutting across all agencies, multiple individuals review the data before it is released to ensure that only individuals with a need-to-know receive the data. This risk cannot be completely mitigated by OPM, however, because the participating agencies retain ownership and control of their file information and records both prior to entry and once the reports are released and it is up to the agencies to ensure appropriate handling of their information.

Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

If individuals wish to access the information about themselves in ESCS, they may contact their employing agency. The agency HR Specialist would then provide access or reach out to OPM ESWD staff for assistance. An individual may also request access by following the process outlined in the OPM/Central-13 SORN and providing the following information for their records to be located and identified: Full name, Social Security Number, and Address where employed. An individual requesting access must also follow OPM's Privacy Act regulations regarding verification of identity and access to records (5 CFR part 297). OPM ESWD will notify the agency of record when an individual makes an access request directly to OPM.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

If individuals wish to correct inaccurate or erroneous information about them that is contained in ESCS, they may contact their employing agency. The agency HR Specialist would then reach out to the OPM ESWD. Individuals may also request a correction by following the process outlined in the Privacy Impact Assessment OPM/Central-13 SORN and providing the following information: Full name, Social Security Number, and Address where employed. Individuals must also follow OPM's Privacy Act regulations regarding verification of identity and access to records (5 CFR part 297).

7.3. How does the project notify individuals about the procedures for correcting their information?

Individuals are notified of the procedures if they contact their employing agency and through publication of the OPM Central-13 SORN and this PIA.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not be able to access their information and request any necessary corrections.

Mitigation: This risk is mitigated by providing a clear process and publishing instructions in the applicable SORN and in this PIA, to inform individuals about how to access and request amendment to their records.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

The database contains log files that capture whenever users access or update (deletions, insertions, and modifications) the system. These log files can be used for auditing purposes if needed. The log files of changes are used for auditing purposes to make sure there haven’t been inappropriate modifications made to the database.

All users are required to sign a new user agreement**.** If they don’t, their account is disabled, and they are required to complete a new user access form and any needed training before the account is re-enabled. Additionally,

OPM leads a cross-agency working group to identify specific reports that may be needed, and the OPM Program Office will be able to ensure that only agency specific, non-PII data is being provided outside of the system. Audit reports are developed and reviewed every 60 days and if users haven't accessed the system in that timeframe their accounts are disabled.

Additionally, role-based access controls and policy controls are employed to limit access to the information by system users based on the need-to-know the information for the performance of their official duties. ECSC also employs processes to enforce separation of duties, to prevent unauthorized disclosure, and to prevent modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees and contractors are required to complete OPM's annual IT Security and Privacy Awareness training. Users for other agencies are required to confirm that they have completed their agency-specific security and privacy awareness training in accordance with agency policy.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

ESCS agency users must have an account to access the system. To receive an account, the user must complete an ESCS OPM Access Request and have it approved and signed by the agency user's supervisor. ESCS users are assigned roles in the application. The role that the user is assigned determines the level of access that user has in the application. For example, some roles can update data where other roles have read only access.

The ESCS OPM Access Request outlines the proper use of the system and what information a particular user is permitted to access. Audits are completed on user login frequency and user accounts that have not logged into within 60 days are disabled. Once an account is disabled, the user must submit a request to the OPM ESWD to have the account re-enabled.

When approved users access the system, a warning message is displayed before the user logs in, stating "This is an official U.S. Government System for authorized use only. Use of this system constitutes consent to security testing and monitoring. Unauthorized use of this system or the information on this system could result in criminal prosecution." Users must explicitly select "Okay" to indicate that they have read and acknowledged the warning message prior to logging into ESCS.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

Any information sharing agreements, MOUs, or new uses of the information must be approved by either the System Owner or the back-up System Owner. Any new uses of the information or new access to the information are reviewed by the OPM ESWD and other agency stakeholders, such as the Chief Privacy Officer and Chief Information Security Officer, as appropriate.

Responsible Officials

Edward Smith
System Owner
Lead Business Systems Specialist

Approval Signatures

Becky Ronayne
Acting Senior Agency Official for Privacy