Privacy Impact Assessment - Summary

MOVEit File Transfer

PRV-2023-130

Department: Cyber Security and Digital Solutions

March 7, 2025

NOVA SCOTIA

1. Basic Information

1.1 Program Area Identifiers

Program or Service Name:	MOVEit File Transfer
Department Name(s):	Cyber Security and Digital Solutions

2. Program or Service Description

2.1 General Description

MOVEit is a managed file transfer service for secure delivery of data from one location to another. The service includes solution engineering for on demand, automated, and advanced transfer requirements. MOVEit, as provisioned by the Department of Cyber Security and Digital Solutions (CSDS), to its client is composed of two services, MOVEit Automation and MOVEit Transfer.

MOVEit Automation is a service that automates file transfers between hosts. MOVEit Automation automatically pulls, processes, and pushes files to any platform, over any network architecture.

2.2 PIA Scope

The PIA reviews both instances of MOVEit Transfer and MOVEit Automation, as provisioned by CSDS, to analyze the privacy impacts and risks associated with the overall system.

2.3 Governance

CSDS is responsible for provisioning the MOVEit service and managing the technical security of the platform. This includes:

- making reasonable security arrangements to protect information transferred using MOVEit
- managing the Master Service Agreement with the vendor, Progress software
- providing technical support for clients

Clients – Public bodies (government departments, agencies, boards, commissions, IWK, NS Health) who have information or communications technology systems and support provided by CSDS. They are the public bodies who will use MOVEit to send or receive packages or files which may contain personal information.

Progress Software – The vendor providing the solution. The relationship is set out in a contract between CSDS and Progress Software. As the vendor, Progress Software provides CSDS with updates, patching, training, and tier two support to resolve issues.

Collection, Use and Disclosure of Personal Information

4.1 Authority for the Collection, Use and Disclosure of Personal Information

The following legislation was reviewed to determine the authority for the collection, use, and disclosure of the personal information related to the MOVEit Service provisioned by CSDS:

- *Freedom of Information and Protection of Privacy Act* (FOIPOP Act)
- *Public Service Act*

Application of Public Service Act (PSA)

Section 46EB(d) of the PSA assigned to the Minister of Service Nova Scotia the supervision, direction and control of all matters relating to information, communication, and technology services for the Government of the Province.

On May 23, 2023, OIC # 2023 – 148 created the Department of Cyber Security and Digital Solutions (CSDS) and assigned to the Minister the supervision, direction and control of all affairs and matters pertaining to information, communication, cybersecurity, and technology services for the Government of the Province. The provision of a file transfer service falls within the scope of these responsibilities.

Freedom of Information and Protection of Privacy Act (FOIPOP)

Governs the collection, use and disclosure of personal information, and provides various provisions regarding how that collection, use and disclosure should be facilitated and under what circumstances it can lawfully occur.

Application of FOIPOP

The authority for collection, use and disclosure of personal information by a government department or a public body is found in sections 24, 26 and 27 of the Freedom of Information and Protection of Privacy Act (FOIPOP Act), which allow for the collection, use and disclosure of authorized personal information that relates directly to and is necessary for an operating program or activity of the public body.

Personal information collected relates directly to and is required to operate CSDS' technology and communications program and authorized by s. 24(1)(c).

Use of Personal Information under FOIPOP

The authority to use the personal information is found in section 26 of the FOIPOP Act. S.26(a) authorizes the use of information by a public body for the purpose it was obtained. The

intended use of personal information is to facilitate the transfer of files to their intended recipients which is the purpose for which it is collected and therefore authorized by s. 26(a).

Disclosure of Personal Information under FOIPOP

A client may use MOVEit to disclose personal information to another department or external third party. While CSDS is using personal information to facilitate the transfer, it is the clients who are choosing the recipient and must consider their authority for disclosures of personal information that may occur as a result.

4.3 Source and Accuracy of the Personal Information

The source of the personal information is the client utilizing the MOVEit service. The client is responsible for ensuring the accuracy of the information in the administration of their programs and the accuracy of the recipient's email either when entering it themselves transfer or when it is provided to CSDS for approved service support.

4.5 Access & Correction Rights

CSDS only collects personal information to facilitate the transfer. No decisions regarding the individual are being made by CSDS. Files are not intended to be retained in MOVEit and files in MOVEit would be treated as duplicates of records held by users. As such users must maintain the personal information for their programs or activities and individuals seeking to access or correct this information should contact the relevant public body that oversees its collection, use and disclosure.

5.4. Information Management

MOVEit is a file transfer system and as such, is not intended to be used as a storage location for files. Clients sending and receiving files are required to manage copies of records in the originating storage systems. By default, files sent using MOVEit are deleted after a standard period of time. The sender has the option to reduce this time. For Folder sharing, the default setting is that files are deleted after 14 days. Standard operating procedures for MOVEit are being developed, which will require clients to request a change in this setting if they wish to keep files in the folder structure for more than 14 days. Approval from an Executive Director within the respective business unit is required for this request. CSDS should consider requiring clients requesting an exception to provide a documented schedule for when files can be deleted from their MOVEit folder sharing.

6. PIA Summary and Findings

6.1 Assessment

The privacy risks associated with using MOVEit file transfer have been evaluated using best practices for risk identification, assessment, and mitigation as described in the IAP Services Writing Privacy Impact Assessments: A Comprehensive Guide. These risks have been rated according to the IT Risk Register framework.

In assessing the impact of the risk, it is not possible to assign a specific rating because the impact will vary based on the nature of the personal information contained in files being sent using the system and the recipient of that information. For example, if an individual has requested records using a FOIPOP request it may contain substantial personal information, such as what might be found in a child in care file from the Department of Community Services (now Department of Opportunities and Social Development). The risk may range from minor to severe if this file is sent to an unintended recipient. As such the impact of a privacy breach to an individual of personal information sent using in MOVEit could range from insignificant to catastrophic.

There were four risks identified in the PIA – broadly, the risks can be themed into two areas: data retention and disclosure risks as well as administrative safeguard risks.

6.2 Strategy for Mitigation of Privacy Risks

Privacy Risk Identification and Mitigation	
Limiting use, disclosure, and retention	
Risk: Personal information within folders may be retained by users beyond default retention period of 14 days, posing a higher risk of being accessed or disclosed.	**Mitigation:** CSDS to finalize process that will require departments requesting an exception to the default time to provide a business case for the longer retention period which will include a schedule for disposition of files in the folder, including naming those responsible for ensuring it is carried out and signed by the business unit's executive director.
Safeguards	
Risk: CSDS may be unable to effectively identify and prevent unauthorized access to, use or disclosure of personal information by those with broad user access	**Mitigation:** CSDS to finalize and document MOVEit audit program and ensure it identifies roles and responsibilities, along with audit type and frequency. CSDS will also ensure the audit program includes monitoring relevant downloads by users with administrator accounts to ensure they are only downloading files from folder structures where there is an operational

such as the administrator role.	need i.e. to provide support to a client who is having issues using their folder structure.
Risk: A package containing personal information may be sent to the wrong recipient, resulting in a privacy breach.	**Mitigation:** CSDS has included directions in FAQs for users on how to retract packages and how to confirm if an attached file has been downloaded and/or viewed.
Risk: Certain tasks on the platform allow full users to see limited personal information that is not necessary for them to know (e.g., name, email address).	**Mitigation:** CSDS will continue to work with the vendor to investigate the possibility of functionality modifications and investigate alternative methods of granting access to external users acting on behalf of public bodies to share documents with different permissions.