Cisco Duo MFA Privacy Impact Assessment

Project Code	PC0945
Submission Date	June 9, 2021
Administrative Authority	Wency Lum, Associate Vice-President University Systems & CIO
Authors and Contact Information	Ryan McRonald, Security Analyst Eric van Wiltenburg, Manager, Information Security Office
Reviewed By	Brad Weldon, Chief Privacy Officer Nav Bassi, Director & Chief Information Security Officer Garry Sagert, Director, UVic Online Services Ron Kozsan, Director, Infrastructure Services
Review Date	June 9, 2021

Purpose: The purpose of the Privacy Impact Assessment (PIA) is to assess risks associated with how a project plans to handle personal information. There are policy and legislative requirements and the purpose of the PIA is to ensure the project approach will be compliant with these requirements, and that any risks to privacy are mitigated or, if they cannot be completely mitigated, understood and accepted by the appropriate Administrative Authority as defined in section 2.00 of Policy IM7800:

> *Administrative Authority means individuals with administrative responsibility for units (e.g., Vice-Presidents, Chief Information Officer, Executive Directors, Deans, Chairs, Directors and other unit heads) and individuals with functional stewardship of university Information Resources.*

Roles:

The role of University Systems is to complete this document and provide guidance regarding security policy compliance and risks to the Administrative Authority.

The role of the Privacy Office is to review this document and provide guidance regarding privacy policy and legislative compliance and risks to the Administrative Authority.

The Administrative Authority is accountable for ensuring the Information Resource being implemented or changed as a result of this project is compliant with privacy and security policies and legislation and accepting risks associated with non-compliance on behalf of the institution.

1.0 Privacy Context

1.1 Description

UVic staff, faculty and students use their Netlink IDs to gain access to university information systems. The Netlink ID and password are at the front-line of protection of UVic's sensitive and personal information.

A compromised Netlink account is one accessed by a person not authorized to use the account. Unfortunately, phishing and other types of attacks that lead to compromised accounts are increasingly common and therefore it is insufficient to rely on passwords alone to protect information.

The Information Security Office Sec. 15 However, the time between compromise and detection can lead to unauthorized access and disclosure of information. Compromised accounts are used for unauthorized access to information, to commit fraud, and to introduce malicious software into our information systems.

UVic's Cybersecurity Program is based on the NIST Cyber Security Framework (CSF). Multi-Factor Authentication (MFA) is an important component of this framework. Internal audit has also recommended MFA to protect institutional information systems. Broad use of MFA for the broader UVic community will be a requirement of our next UVic Information Security Standard (A6.7). While Yubikey hardware tokens have been effective MFA solution for small sets of users, it does not scale well to the size and nature of our user community.

The purpose of this privacy impact assessment is to see that our implementation of Cisco Duo ("Duo") for MFA is compliant with BC's *Freedom of Information and Protection of Privacy Act* (FIPPA). Duo is a service that provides additional layers of security designed to protect access to our secure applications and services. It is a cloud-based authentication solution. We want to maximize adoption of MFA by our community by making it available to all of our authorized and licensed users.

Duo is compatible with a broad range of user devices, as well as our existing CAS single sign-on. Duo is deployed at UofT, UBC, uWaterloo, and according to our research is the most prevalent MFA solution in use by North American Universities and Colleges.

Instances of Duo can be installed in Amazon Web Services (AWS) Canada where its data remains within Canada. However, this would come at a cost of reduced functionality as described later in this PIA. Fully functional versions of Duo reside in AWS global locations and are not fully contained inside of Canada.

Duo will be available to protect certain applications (e.g. CAS single sign-on Outlook Web Access) used by all types of users including staff, faculty, and students. The roll-out will be subject to meeting our compliance obligations such as completing this PIA. Determining which applications will use MFA, and whether MFA will be mandatory or not, will be determined by risk assessment and consistency with our policies and standards and approvals by the appropriate authorities.

Today most applications only require a username and password to succeed at login. When protected with Duo, the username and password will be verified with our existing password infrastructure before triggering Duo's policy-driven workflow. Except for command line environments, the first step is to check the security of the user devices. Our policy determines how we block, notify, or restrict access to users with risky devices. The next step requires the user to take additional action (e.g. confirming login via Duo's mobile app, transcribe an SMS, answer a phone call, transcribe digits from a hardware token, etc.) before the login process can be completed. Our policy will control which internal applications are accessible by which groups of users.

It is important to note that when implemented Duo will be an essential control in the protection of the personal information managed by UVic eventually across its information systems.

1.2 Privacy Issues Related to this Project

Users will need to provide personal information to Cisco in order to use the MFA service. In some cases (e.g. staff) this may be limited to business contact information, which is not personal information under FIPPA. In other cases (e.g. students), this will include personal information covered by FIPPA. The privacy issues related to this project are:

1. **Reasonable Security Measures**: FIPPA section 30 requires public bodies to employ reasonable security measures against risks to personal information. The primary goal of implementing MFA is to reduce information security risk to personal and UVic information, including unauthorized access, collection, use, disclosure or deletion of information, in direct support of FIPPA. The Duo solution adheres to stringent information standards including the US Federal Risk and Authorization Management Program (FedRAMP) standard for cloud service providers.
2. **Storage and access to personal information outside of Canada**: potential privacy issues related to storage of information outside of Canada will be mitigated by;
    a. minimizing the amount of personal information required to be disclosed to Cisco to that which is unlikely to be of interest to US law enforcement;
    b. provide the user with the option to use a physical MFA key as an alternative installation of the Duo MFA smartphone application;
    c. notify users about how the information to be stored outside of Canada will be protected; and
    d. seek user consent for the disclosure of personal information outside of Canada.
3. **Metadata storage and access to personal information outside of Canada**: potential privacy issues in this area involve metadata with a privacy interest. We will mitigate these potential issues by appropriately protecting this metadata.
4. **User awareness**: a user's choices will influence what personal information is involved and therefore users need to be informed about how and consent to their choices.

More information on these issues and mitigations is provided throughout this PIA.

1.3 Privacy Impact Assessment Scope

The solution's scope areas resulting in records to be managed under MFA are:

Solution Scope	Privacy-Related Activities and Processes
Mobile device "App" installation	Collection of metadata surrounding the installation of the Duo App.
Account registration & account update	Collection of personal information as required to support the user registration and the factor registration processes.
End user authentication	Collection of authentication event metadata and use of the previously collected registration data.
Account de-provisioning	Archiving and eventual deletion of information when no longer required.

1.4 Related Privacy Impact Assessments

No other privacy impact assessments have been completed in relation to MFA.

1.5 Elements of Information or Data

The elements of information to be collected, used, disclosed, and disposed of in relation the Duo solution are described in the following table. The information collected by the solution depends upon two factors:

1) **The "edition" and functional configuration of Duo**: Cisco offers "editions" of its software referred to as "User Trust", "Device Trust", and "Adaptive Authentication & Policy Enforcement". Each subsequent edition requires additional information to perform its services. "User Trust" is the most basic level and only requires account information (e.g. username and email address). "Device Trust" adds device information in order to enforce its policies based on the device's attributes. "Adaptive Authentication & Policy Enforcement" is the most sophisticated edition and require information such as geographic location in order to enforce its policies based on a user's location

"Adaptive Authentication & Policy Enforcement" is the edition of Duo that is currently not fully contained within Canada. Currently there is no plan to license the "Adaptive Authentication & Policy Enforcement" edition but this PIA is being conservatively written based on the capabilities offered by this edition.

2) **The type of device(s) a user chooses to register with Duo**: Duo enables a user to register a variety of factors. The user will have a choice to register either:

1. a Time-based One-Time Password (TOTP) token; or
2. the Duo "App" for Android or iOS

The factor involving the least personal information is a Time-based One-Time Password (TOTP) token. The factor involving the most personal information is "push" notifications enabled through the Duo App based mobile devices.

In summary, the information collected depends upon the user and their actions. It is important to note that this PIA is based upon the most extensive possible cases of information collection, use, disclosure, and disposal. It is important to note that the user's choices will determine what information is collected and have the option to use the TOTP token to minimize disclosure of personal information outside of Canada. Therefore, it is an important aspect of this solution that users are provided with options and provided with clear information on the choices they make in relation to their information insofar as personal information is involved.

Information or Data	Description	Usage	Classification
End Users			
Account information	• Username • Telephone number (optional) • Email address • Organization name This is the minimum amount of personal information that must be disclosed outside of Canada.	• Account creation and activation • Service authentication and login • Deliver, support, improve security functionality, upgrade, and improve the services	In some cases (e.g. staff with a UVic provided device) this may be limited to business contact information. In other cases (e.g. students), this may include personal information and will require consent.

End User Metadata	• Device type • Device operating system, device version, and other device characteristics (e.g., if a device is "jailbroken" or has a screen lock in place) • Connection information - such as encryption protocol(s) being used to access the Duo service • Browser type • IP address • Whether a Public Key Infrastructure Certificate is installed • Time zone • Time and date of authentication • Broad geographic area (country or city-level location) • Application that device is attempting to access • Whether device is utilizing certain plugins • Device identifiers (e.g., device name, processor ID, serial numbers, UDIDs, UUIDs, DNS Hostname)	• Provide and maintain the services • Improve user experience • Improve security functionality • Improve quality of the services • Ensure secure devices and/or applications • Issue certificates verifying device is secure • Authenticate device • Conduct statistical analysis with pseudonymized and/or aggregate usage data to improve the services • Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, security risks, etc.	While this information is not personal information there is an established 'privacy interest' in such metadata.
Administrators			
Duo Administrative account information	• Username • Telephone number • Email address • Billing and delivery address • One-way hashed representations of password(s) for the Duo Administrator Panel • Job title • Organization name	• Account creation and activation • Service authentication and login • Deliver, support, improve security functionality, upgrade and improve the service	In all cases (i.e. staff) administrative account information should be business contact information. However, the possible but unlikely opportunity exists for the user to enter personal information such as personal telephone numbers.
Log Data			
Events and Usage Data	• How end-users access the services • Dates and times of access	• Provide and maintain the services • Improve user experience	While this information is not personal information there is an

	• IP address for determining where the services are accessed • Device events (e.g., crashes, system activity, hardware settings)	• Improve security functionality • Improve quality of the services • Conduct statistical analysis with pseudonymized and/or • aggregate usage data to improve the services • Prevent, detect, respond and protect against potential or • actual claims, liabilities, prohibited behavior, security risks	established 'privacy interest' in such metadata.
Authentication and Activity Logs		• Provide and maintain the services • Improve user experience • Improve security functionality • Improve quality of the services • Conduct statistical analysis with pseudonymized and/or • aggregate usage data to improve the services • Prevent, detect, respond and protect against potential or • actual claims, liabilities, prohibited behavior, security risks	While this information is not personal information there is an established 'privacy interest' in such metadata.

The information in this table was adapted from Cisco's Privacy Data Sheet. The Sheet's purpose is to assist Cisco's customers to understand the information collected and used by the Duo solution. Many of the information types in the table might not be intuitively recognizable as personal information. However, the Privacy Commissioner of Canada's Technical and Legal Overview of Metadata identifies a "strong privacy interest" associated with many of the types of metadata involved, and in several cases, Canadian Courts have identified that these types of information deserve privacy protection.

2.0 Protection of Personal Information

2.1 Storage or Access outside of Canada

Fully functional instances of Duo's "Adaptive Authentication & Policy Enforcement" edition reside in Amazon Web Services (AWS) Global both inside and outside of Canada. Instances of Duo could be installed in Amazon Web Services (AWS) within Canada. However, this would come at a cost of reduced functionality and the loss of Duo's "Adaptive Authentication & Policy Enforcement" functionality. For this reason this PIA must address the topics of storage and access to personal information outside of Canada.

2.2 Personal Information Flow Diagram and/or Personal Information Flow Table

The flows of information and metadata are as follows:

Note that this flow examines the sequence of events which involves the most personal information. If the user chooses to register a TOTP token instead of using the Duo App, then user-related information is collected or used but device information is not collected or used.

The flows of information, type, and authorities are as follows:

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	**Registration**: where device-related and user-related information and metadata are collected for the purposes of registering the user for the Duo service.	Collection & disclosure	S26 (c) that the information relates directly to and is

	In cases where self-service is used, the collection is between the student and Cisco. UVic is not responsible for this collection. In exceptional cases (e.g. problem resolution) where administrative tools are used to register the user or the user's device, the collection is between the student and UVic. Then UVic discloses this information to Cisco as permitted under FIPPA 33.1(1)(p)(i)(A).		necessary for an operating program or activity of the public body. s. 26(a) authorized by the *University Act* s. *33.1 (p) necessary for* installing, implementing, or trouble-shooting an electronic system. s. 33.1 (b) disclosure outside of Canada with consent
2.	**On-going use**: where device-related and user-related information and metadata are collected and used for the purposes of authenticating the user with the Duo service	Collection & use	S26 (c) that the information relates directly to and is necessary for an operating program or activity of the public body. s. 32(a) use for the purpose the information was obtained or compiled
3.	**Disposal**: where device-related and user-related information and metadata are disposed when no longer required	Disposal	S30 retention of the minimum amount of time necessary

2.3 Risk Mitigation Table

The following privacy risks and mitigation strategies have been identified and assessed:

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Personal information is included in automated response actions	A limited retention time of Sec. 15 helps mitigate this risk. Cybersecurity awareness training minimizes the likelihood of incidents. Review this	Low	Low

	from Duo when it should not or no longer be available.	collection with the CPO to ensure collection of PII is not excessive.		
2	Personal information is retained in old logs	A short retention time of Sec. 15 helps mitigate this risk. Cybersecurity awareness training minimizes the likelihood of incidents. Review this collection with the CPO to ensure collection of PII is not excessive.	Medium	Low
3	Unauthorized interception or access to internal or confidential data in Duo.	Cisco has strong privacy and security controls in place, including encryption. UVic provisioning procedures and policies will protect access to the system.	Low	Low
4	Log data retention beyond the configured retention period.	The maximum retention period possible is Sec. 15. Data in Duo will be purged after the maximum retention period.	Low	Low
5	Account data retention beyond the account lifespan	Accounts will be de-provisioned automatically as part of the account lifecycle	Low	Low

3.0 Security of Personal Information

3.1 Please describe the physical security measures related to the initiative (if applicable).

Cisco has periodic independent audits to verify that Duo adheres to security controls for ISO 27001, ISO 27018, SOC 2, Federal Risk and Authorization Management Program (FedRAMP), EPCS, and NIST Cryptographic Certifications such as FIPS 140-2. Many of these standards include physical security measures as appropriate for confidential and personal information. For example, the FedRAMP (Moderate) standard includes requirements for security assessment, authorization, and continuous monitoring for cloud products and services to be used by the US government. That standard includes Physical and Environmental Protection (PE) controls which periodic reviews and audits confirm are in place.

3.2 Please describe the technical security measures related to the initiative (if applicable).

Duo has maintained uptime of greater than 99.99% for more than four years backed by Service Level Agreements (SLAs). Duo's servers are hosted across independent PCI DSS, ISO 27001-certified, and SSAE 16-audited service providers with strong physical security. Cisco provides a high-availability service split across multiple geographic regions, providers and power grids for failover. Multiple offsite backups are encrypted.

3.3 Does your department rely on security policies other than the Information Security Policy?

Other than the Acceptable Use Policy IM7200, no other security policies are involved.

3.4 Please describe any access control and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Access to the Duo portal is restricted to administrative accounts. By policy, accounts that are granted access to the portal requires multi-factor authentication. Within the Duo console, Role Based Access Control (RBAC) is used to delegate administration and limit access to the necessary level for each user.

Provisioning and de-provisioning procedures will be followed for granting access or removing access to the Duo portal. Access will be limited to a small number of qualified personnel within University Systems.

Duo personnel access is limited by controls they have in place to prevent any abuse of access. This includes tight access controls to sensitive data, background verification checks, and a formal process when they are required to access a customer's account or related information in the performance of their duties.

3.5 Please describe how you track who has access to the personal information.

Administrative access is logged in the Duo solution. All user actions in the Duo console are tracked in audit logs for each machine and can be retrieved if necessary within the Sec. 15 day retention period.

4.0 Accuracy/Correction/Retention of Personal Information

4.1 How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the university notify them of the update, correction or annotation?

Device-related metadata and user-related personal information is collected at registration. A user can update their own information through the Duo portal. An authorized administrator can update a user's information through the Duo portal.

4.2 Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

No decisions on entitlements or benefits use this personal information. The personal information is used for the purposes of establishing and utilizing the MFA service.

4.3 If you answered "yes" to question 4.2, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

The management of personal information will primarily occur through self-service. A user can update their own information through the Duo portal. In exceptional cases where self-service is not possible an authorized administrator will update a user's information through the Duo portal.

4.4 If you answered "yes" to question 4.2, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

No records retention or disposition schedule for authentication records is currently in force.

5.0 Further Information

5.1 Does this initiative involve systematic disclosures of personal information? If yes, please explain.

No, information sharing agreements are not applicable to the Duo solution.

Information Sharing Agreement – Required Information	
Description	*n.a.*
Primary department involved	
All other departments involved	
Business contact title	
Business contact telephone number	
Indication of whether or not personal information is involved	
Start date	
End date (if applicable)	

5.2 Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No

5.3 Will a personal information bank (PIB) result from this initiative?

No

5.0 Comments and Signatures

Associate Vice-President University Systems & Chief Information Officer: Wency Lum
(Also the Administrative Authority)

Comments:	
Date:	
Sign-Off:	

Portfolio Manager: Nav Bassi, Director & Chief Information Security Officer

Project Comments:	**Multi-Factor Authentication is a critical security control that must be implemented to manage information security risk at an acceptable level and meet our requirements to ensure reasonable security of personal information under FIPPA. Cisco Duo offers the best solution for our community.**
Date:	June 9, 2021
Sign-Off:	Electronic

Consultation Checklist

IT Projects

The following leaders in each functional area can refer you to an appropriate subject matter expert to help develop the technical elements of your project plan and ensure it is complete.

Service Area	Impact? (Y/N)	Leader	Expert Consulted	Date of Consultation
Senior Management				

Associate Vice-President University Systems and Chief Information Officer		Wency Lum		
Director, Academic & Admin Services, and Chief Information Security Officer		Nav Bassi	Y	June 9, 2021
Director, Infrastructure Services		Ron Kozsan	Y	June 9, 2021
Director, UVic Online Services		Garry Sagert	Y	June 9, 2021
Academic & Administrative Services and Information Security Office				
Client Technologies		Lance Grant		
Computer Help Desk		Marcus Greenshields		
Desktop Support Services		David Street		
Information Security Office		Eric van Wiltenburg		2021-05-17
Infrastructure Services				
Data Centre Services		Kim Lewall		
Network Services		Jane Godfrey		
Research Computing Services		Ryan Enge		
UVic Online Services				
Development Services		Ivan Petrovic		2021-05-17
Production and Technical Support		Rizwan Bashir		
Project Management Process and Budget				
Administrative Officer		Trish Kearley		
Project Management Office		Scott Thompson		
Other Consultations				
Privacy Office		Brad Weldon		2021-06-07
[Department/Unit]		[Expert Consulted]		

Revision History

Version	Date	Author	Comments