Subject: Keeping Your SSO Secure

Dear Single Sign On (SSO) User:

SSO will **require two factor authentication (2FA)** for all logins beginning **May 15, 2019**. This change helps make SSO more secure, safeguarding your information in Workday, Canopy, HRConnect, Business Objects and other applications.

Two factor authentication provides a second layer of security to your accounts. Our network is maliciously attacked every day from phishing scams, shared passwords or malware. By enrolling in two factor authentication through Duo, you will have re-assurance that your accounts are secure.

1. Login to SSO
2. Click the 'Profile' tab from the top menu
3. Select 'Two Factor Authentication' from the left menu to begin your enrollment

You can choose from one of three authentication methods:

Method	Description
Duo Push	• Pushes a login request to your phone or tablet (if you have Duo Mobile installed and activated on your iOS, Android, or Windows Phone device). Just review the request and tap **Approve** to log in ***(recommended method)***
Call Me	• Authenticate via phone callback (such as your office phone)
Enter a Passcode	• Login using a passcode, generated with Duo Mobile, sent via text message • Click Send codes to get a new batch of passcodes texted to your phone

If you need any assistance, please contact your SSO Department or Central Administrators on the 'Contact' tab from the SSO top menu.

Thank you for helping keep your data and our network safe!

System Enterprise Applications
Office of Information Technology
The Texas A&M University System