DGS CALIFORNIA DEPARTMENT OF GENERAL SERVICES

HUMAN RESOURCES MEMORANDUM 23-007	DATE ISSUED: 5/22/2023
SUBJECT: **MULTIFACTOR AUTHENTICATION (MFA) FOR CAL EMPLOYEE CONNECT (CEC) ACCOUNT**	REFERENCE: California Employee Connect (CEC)
TO: All DGS Employees and Client Service Agencies.	SUPERCEDES:

PLEASE ENSURE THAT THIS INFORMATION IS SHARED WITH YOUR EMPLOYEES

Purpose

In light of recent security incidents occurring within California and around the world, it is more important than ever for state employees to secure their Cal Employee Connect (CEC) account, as well as all personal online accounts against unauthorized access.

With an increase in suspicious personal account activity due to weak and/or reused passwords, as well as the same user IDs being used across multiple online accounts, the State Chief Information Security Officer (SCO) highly recommends state employees take immediate action to secure personal identifiable data.

CEC offers secure Multifactor Authentication (MFA) through an Authenticator App downloaded to your smartphone. Authenticator Apps are applications that authenticate your identity by generating a unique code that must be used in addition to your username and password to access your CEC account.

In order to provide an extra layer of security to your CEC account, SCO encourages you to set up MFA as soon as possible.

Steps to Enable Multifactor Authentication

1. Log into Cal Employee Connect[1] (CEC) and turn on Multifactor Authentication (MFA).
    a. When logging into your CEC, please use a different device other than your personal smartphone. The reason for this is that you will be required to scan the QR Code using your phone's camera.
2. You will be prompted to download an authenticator application of your choice to your smartphone. The app should be installed on your personal phone rather than your work phone.
    a. If you do not yet use an authenticator app on your smartphone, you must install one through the respective app store (ex. Google Play or Apple Store). SCO recommends the Google Authenticator or Microsoft Authenticator.
    b. **IMPORTANT:** Once you download the Authenticator App to your smartphone, **DO NOT DELETE THE APPLICATION.**
    c. If you have both a personal and work phone, you should enable MFA using your personal smartphone. The reason for this is if you move to another

agency and lose access to your existing work phone, you could be locked out of your Cal Employee Connect account.

3. Open the Authenticator App you installed.
4. Scan the QR Code using your phone's camera. The authenticator app will generate a six-digit verification code. Enter the six-digit verification code into CEC and click "Enable."

Questions

Employees are encouraged to view the **Enable MFA User Guide** for additional instructions.

If employees have questions, need further assistance, or want share feedback, please visit CEC Help and Feedback[2].

[1] https://connect.sco.ca.gov/
[2] https://connect.sco.ca.gov/help

ESTELA GONZALES, Chief
Office of Human Resources