

## HOW TO CONFIGURE CAC READER FOR MAC

This instruction sheet will go over on the configuration steps for allowing your CAC reader to access OWA and SOUTHCOM's portal.

Prerequisites and caveats.

- Recommended browser to use is Microsoft Edge or Google Chrome. You can use Firefox but that will take additional steps that are outlined in [homecacuse.com](http://homecacuse.com).
- Make sure your iOS is up to date.
- Have CAC reader plugged in with your CAC inserted.
- First part of instructions will explain on getting OWA Email access and the second will explain NIPR Portal Access
- When you are done with your session, take your PIV and unplug your CAC reader.

1. Go to URL: <http://homecacuse.com/> and click on 'Install for Mac'.



The screenshot shows the homepage of HOME CACUSE .com. The logo is at the top left, featuring a stylized CAC reader icon. A dark navigation bar contains the following links: Home, Install For Mac, Install for PC, Best CAC Card Readers, Blog/CAC Reader Reviews, and Contact. Below the navigation bar is a main content area with a large image of a family (a woman, two children, and a man in military uniform) and the text "Learn How To Install Your Home CAC Reader In Minutes!". Below this is a section titled "Get Started With Your CAC Reader Now!" which contains three buttons: "Best Readers" with a CAC reader icon, "Install For Pc" with a Windows logo, and "Install For Mac" with an Apple logo. The "Install For Mac" button is highlighted with a red border. To the right of the main content is a "Menu" section with links to Home, Install For Mac, Install for PC, Best CAC Card Readers, Blog/CAC Reader Reviews, and Contact. Below the menu is a disclaimer: "We are a participant in the Amazon Services LLC Associates Program, an affiliate advertising program designed to provide a means for us to earn fees by linking to Amazon.com and affiliated sites."

2. Scroll down to Step 3 and download all the certs in the red box. After downloading, double click each one of them. If you prefer to use Firefox, please follow the additional steps below.

### Step 3: Update Your DOD Certificates

Now that you have your CAC reader connected and accepted on your Mac computer, it's time to ensure you have the right certificates in order to access DOD CAC required web pages.

#### Procedure for Chrome and Safari

1. Type  $\text{⌘}+\text{U}$  (Shift + Command + U) to access your Utilities
2. Find and Double click "Keychain Access"
3. Select "Login" and "All Items"
4. Download the following four files and double click each once downloaded so as to install in your Keychain Access

1. Mac All Certs
2. Mac Root Cert 2
3. Mac Root Cert 3
4. Mac Root Cert 4

5. When you double-click the Mac Root Cert 3 and 4, you'll need to tell your browser to always trust them. Click the button like you see below:

#### Additional Steps for Firefox

If you're using Mozilla Firefox as your primary browser, you're going to need to perform some additional steps. First, perform the same steps that you did for Chrome and Safari. Afterwards, follow these additional steps to get started.

1. Download All Certs zip and double click to unzip all 39 files
2. While in Firefox, click "Firefox" on the top left, then "Preferences"
3. Then Click "Advanced" > "Certificates" > "View Certificates"
4. Then Click "Authorities" and then "Import"
5. Import each file individually from the "AllCerts" folder. When you do this, the below box will popup. Check all three boxes and click "OK"

### Step 4: Download and install CAC Enabler

1. Download zip
2. Double click the .zip file
3. Because this is from an unidentified developer, you'll need to hold down "Control" and click the program. Now select open and continue with install procedure.
4. After installing, restart your computer

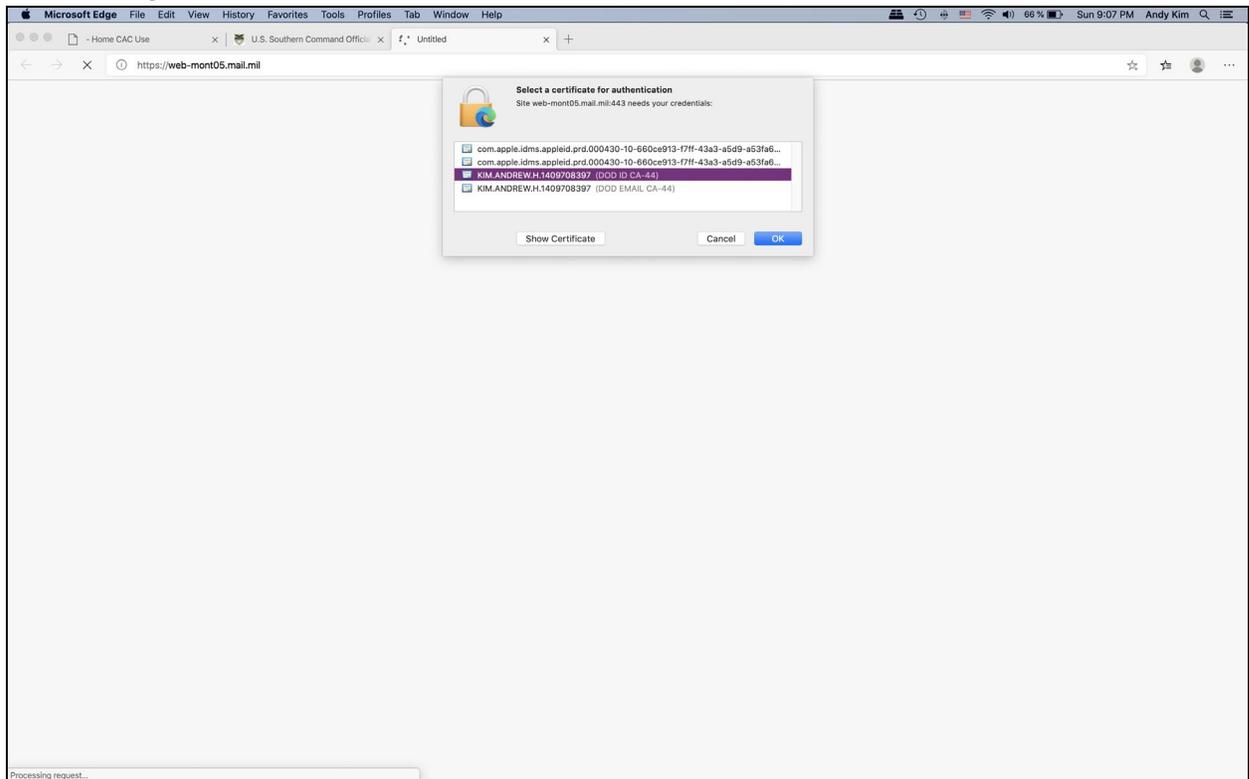
### CAC Access at Home Success

Now that you have a CAC reader, certificates, and a CAC Enabler, you should now be able to access any CAC-enabled website and log on using your CAC password and data.

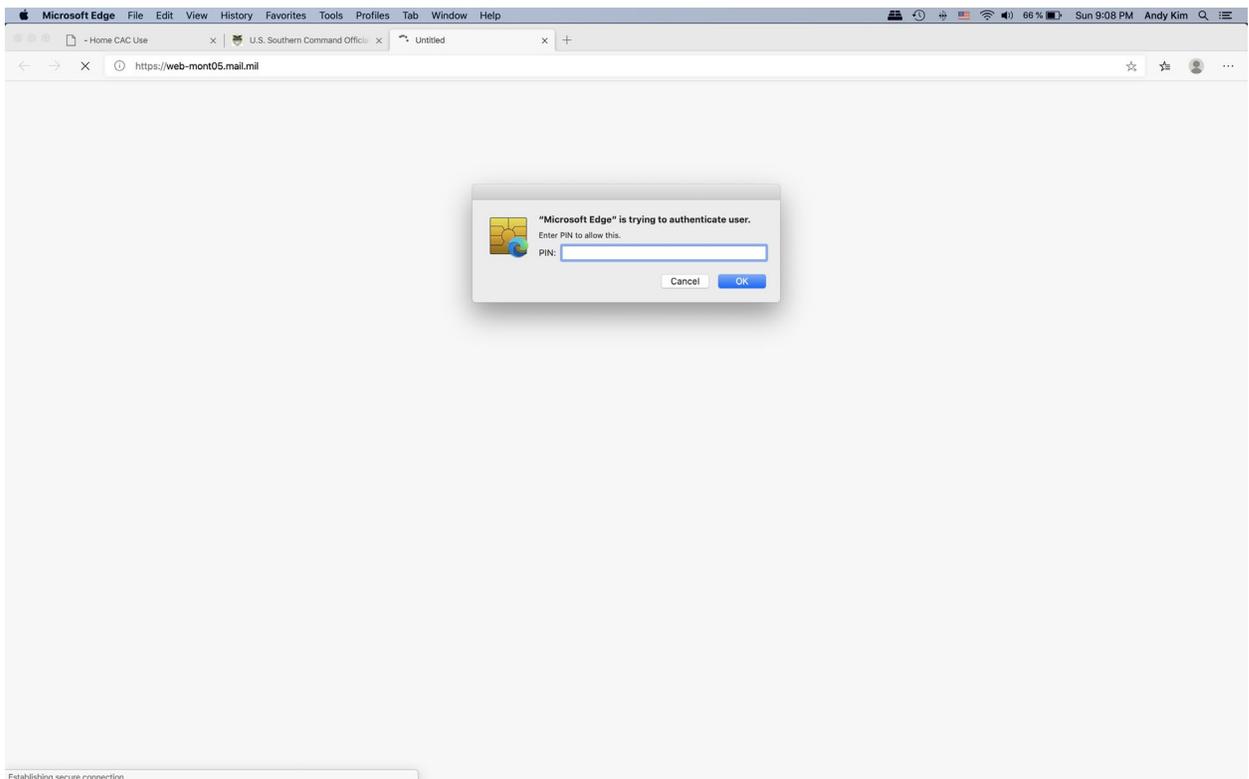
3. Go to URL: <https://www.southcom.mil> and scroll down until you see DEE Webmail – CAC Access and click on it.

The screenshot shows the Microsoft Edge browser displaying the Southcom website. The address bar shows the URL <https://www.southcom.mil>. The page content includes a 'STAY CONNECTED' header with social media icons, followed by three main columns: 'SOUTHCOM COMPONENTS', 'SOUTHCOM TASK FORCES', and 'SOUTHCOM ACCESS'. Under 'SOUTHCOM ACCESS', there is a section for 'PORTALS & COLLABORATIVE SITES' where the link 'DEE Webmail - CAC Access' is highlighted with a red box. Other links in this section include 'NPR/Internal Portals' and 'AFAN (All Partners Access Network)'. Below this, there are sections for 'SITES OF INTEREST', 'EQUAL OPPORTUNITY (EO) OFFICE', and 'EQUAL EMPLOYMENT OPPORTUNITY (EEO) OFFICE'. At the bottom, there is a 'QUICK LINKS' section with various utility links and a 'SEXUAL HARASSMENT ASSISTANCE & RESPONSE CENTER SHARP' logo with a phone number (805) 753-5923.

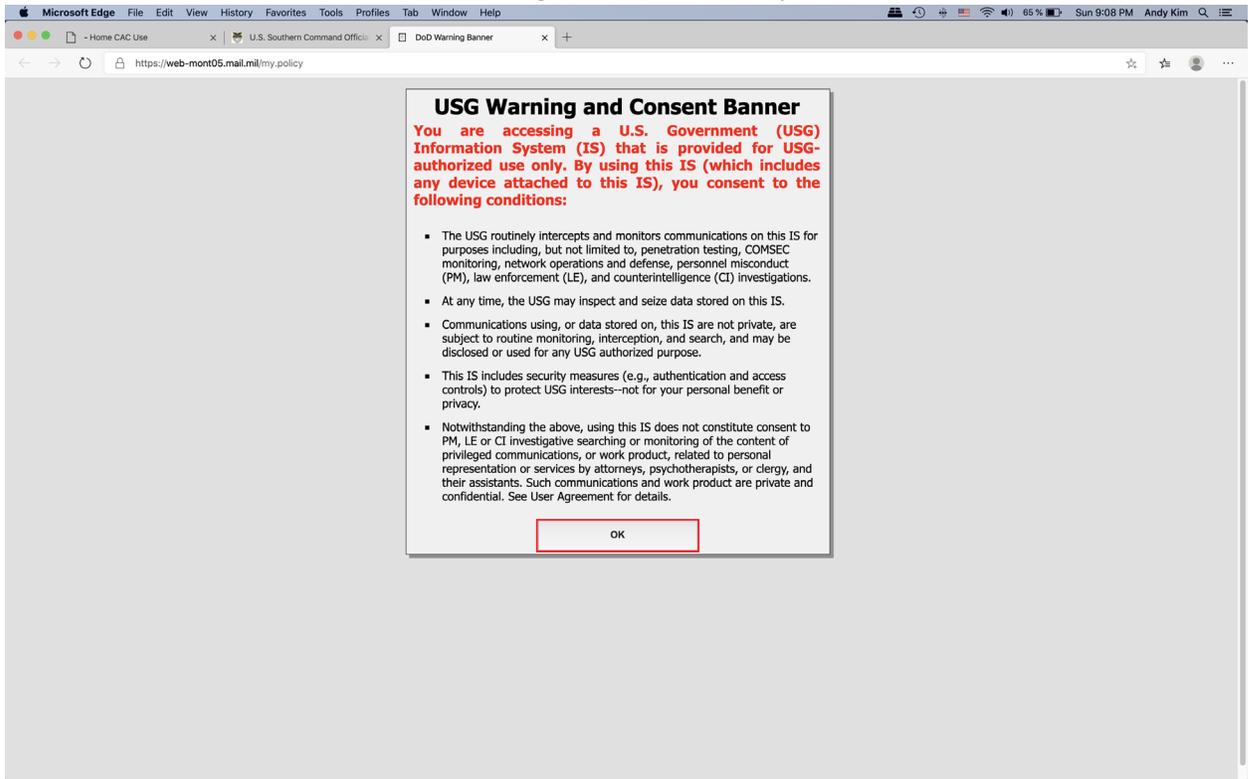
4. After clicking on DEE Webmail – CAC Access, select (DOD ID CA-44) certificate and click ok.



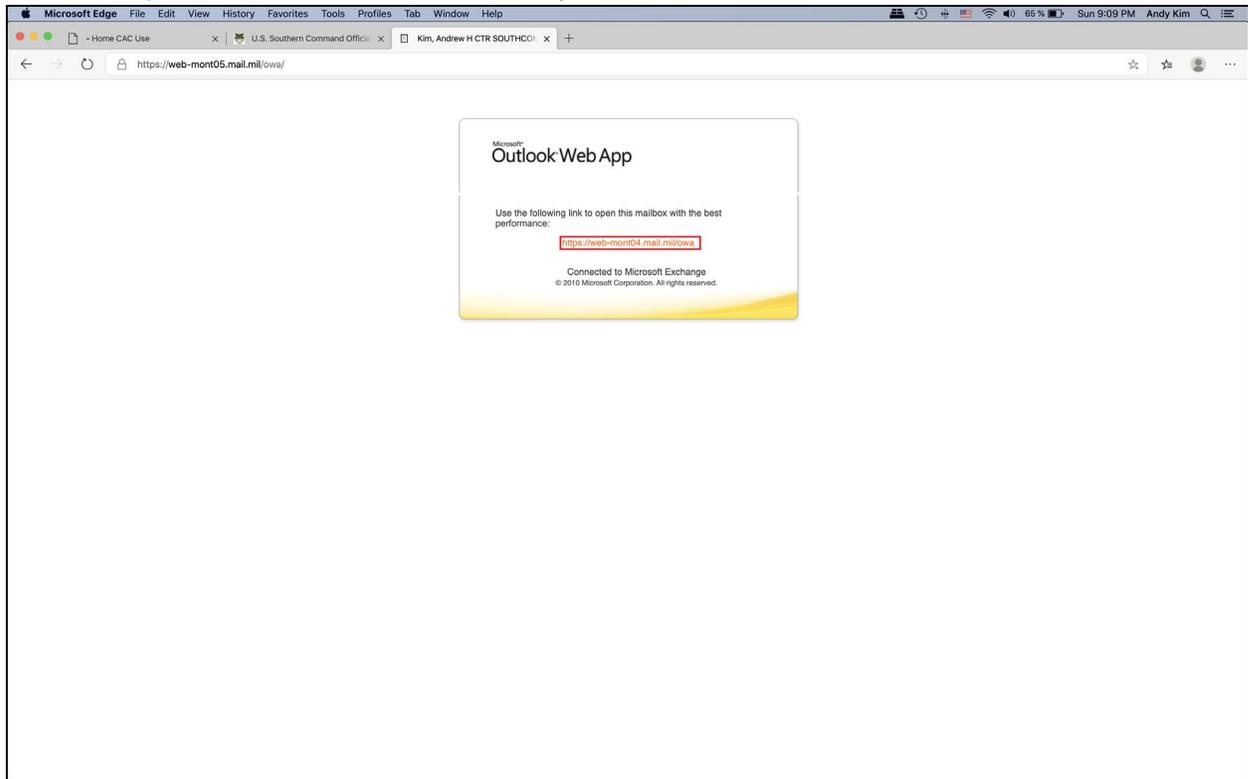
5. After clicking on OK, enter your PIN and click Ok.



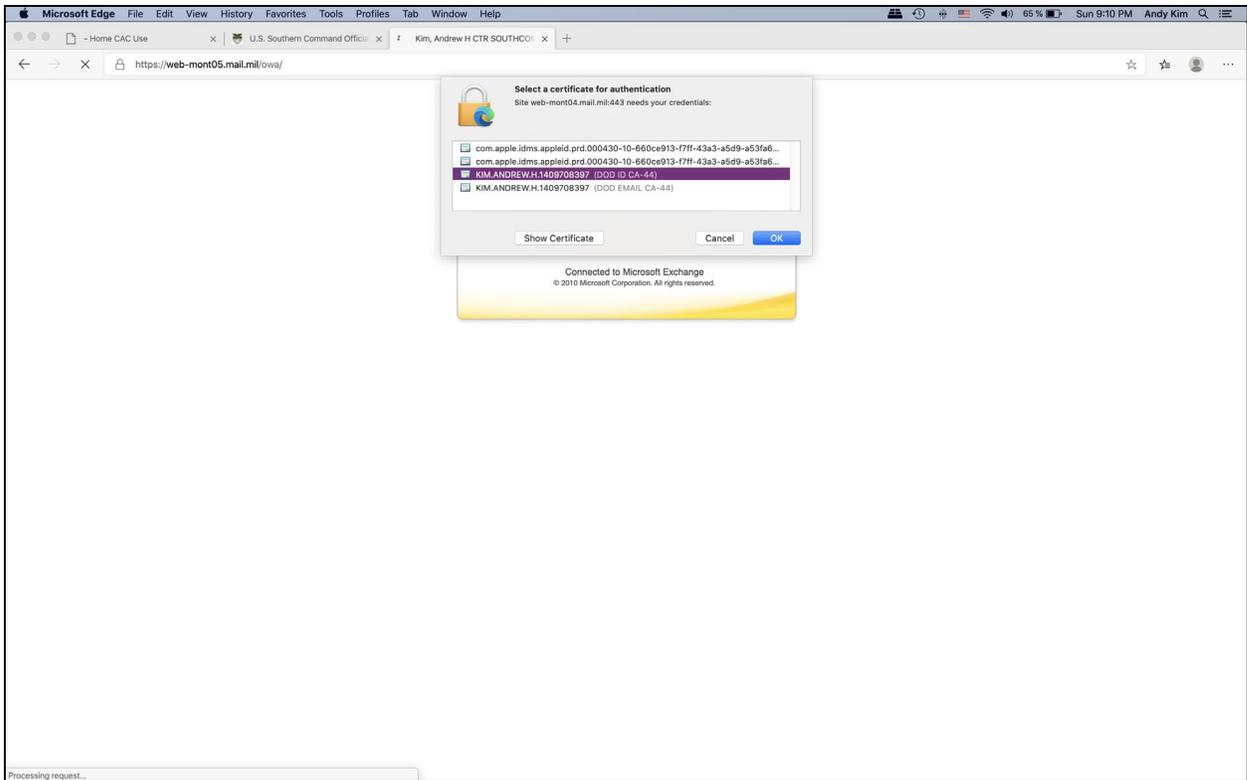
6. You will now be directed to the DoD Warning Banner, click ok to proceed.



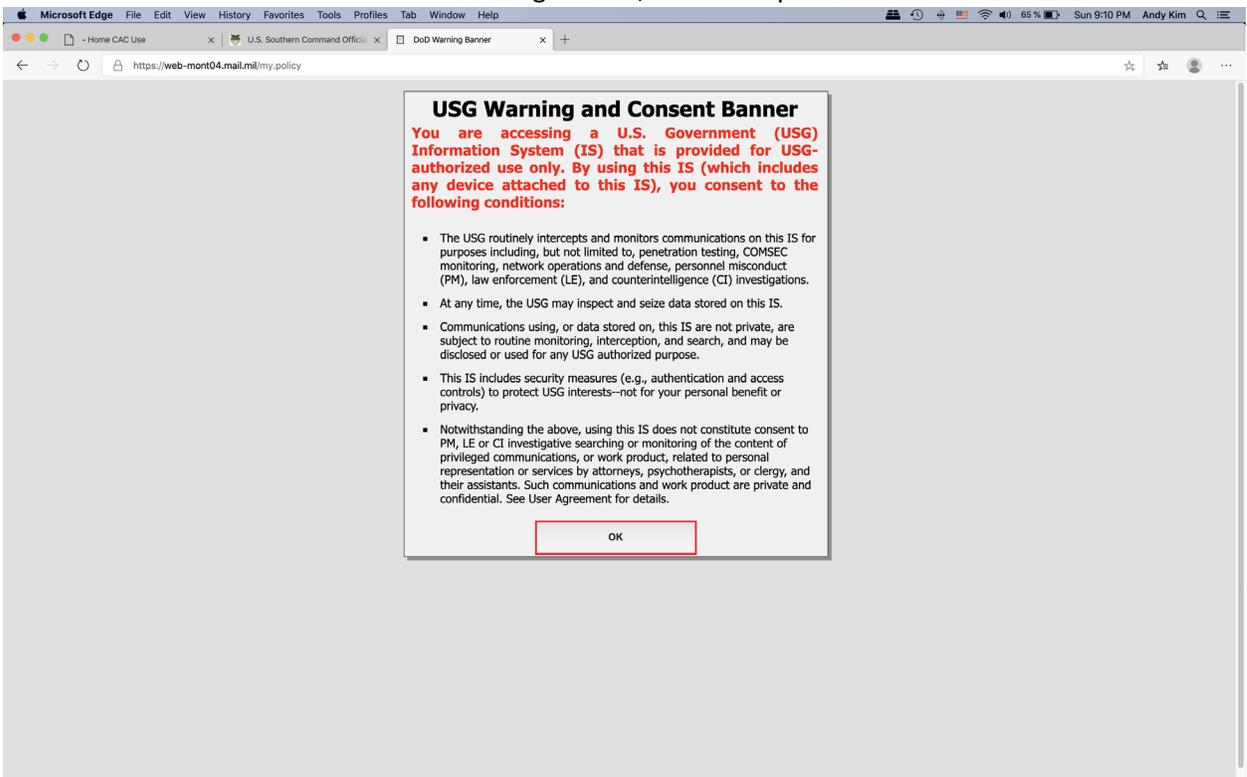
7. Click on <https://web-mont04.mail.mil/owa> to proceed.



8. Select (DOD ID CA-44) certificate and click ok.



9. You will now be directed to the DoD Warning Banner, click ok to proceed.



10. You will now be in Outlook Web App.

The screenshot displays the Outlook Web App interface in a Microsoft Edge browser window. The address bar shows the URL <https://web-mont04.mail.mil/owa/>. The page title is "Outlook Web App" and the user is logged in as "Kim, Andrew H CTR SOUTHCOM 7 SIG CMD".

The left sidebar shows the navigation pane with "Mail" selected, displaying "Inbox 9784 Items". The main content area shows a list of emails, with the selected email titled "Command Update: Building Our Team Email # 41 (UNCLASSIFIED)" from "Faller, Craig Stephen ADM USN SOUTHCOM SC-C...".

The email content is as follows:

**Command Update: Building Our Team Email # 41 (UNCLASSIFIED)**

**Faller, Craig Stephen ADM USN SOUTHCOM SC-CC (USA)**

To: SOUTHCOM Miami SC-CC DDL USSOUTHCOM HQ Only, SOUTHCOM Miami SC-CC List ALL SC COMP-CDR  
Cc: SOUTHCOM Miami SC-CC List All Executive Officers; SOUTHCOM Miami SCJ2 List Parents Support Group; USARMY Miami USAG List ALL GARRISON; USMC Miami MARFORSOUTH-CG List All Hands; usouthcom.sfr@gmail.com

Sunday, March 22, 2020 10:29 PM

CLASSIFICATION: UNCLASSIFIED

Teammates,

I personally know the tremendous stress this crisis places on all of you and your families. Social distancing, working from home and medical isolation can lead to a loss of spirit and loneliness. Please know that you are not alone. Together we will succeed.

**UPDATES: No member of the SOUTHCOM team has tested positive to date.** This includes from the 8 March Brazilian delegation visit. Not all test results are back yet and today is the 14<sup>th</sup> day. It's important to note that we offered testing in an abundance of caution and we were actually being more conservative than recommended testing guidelines. As such, if you were present Sunday 8 March, self-isolated and are showing no COVID-19 symptoms, you may come out of self-isolation. If in doubt, consult health care professionals. As a reminder, we remain at essential manning only at our HQ.

We have one J-8 person (not connected to the 8 March event) who is awaiting test results based on symptoms. Last time this person was in the HQ building was 13 March. We deep cleaned all affected areas. We used our security camera system to map this person's path and contacts. All people known to have close contact with this individual on 13 March have received individual outreach.

Going forward it's important we continue to demand telework, flex hours and shift work. Leaders must review every contract to ensure contracts are amended to require only min essential people at work. Chief of Staff will publish additional guidance on work place protocols.

We continue to work with the Department of State to facilitate the transport of DOD/USG personnel and AMCITS back to the United States. Below my signature you will find more information on what to do if someone reaches out to you or your team with a lift request.

We are at war with COVID-19 and we must balance the sense of urgency required to fight this with the knowledge that this is going to be a long duration campaign.

Best info: CDC – COVID-19 Virus  
<https://www.cdc.gov/coronavirus/2019-ncov/index.html>

<https://www.southcom.mil/coronavirus/> Starting tomorrow our chaplains will post resiliency notes. Our chaplain team can be a resource – please use them.

Be well, stay informed, be calm and ask questions.

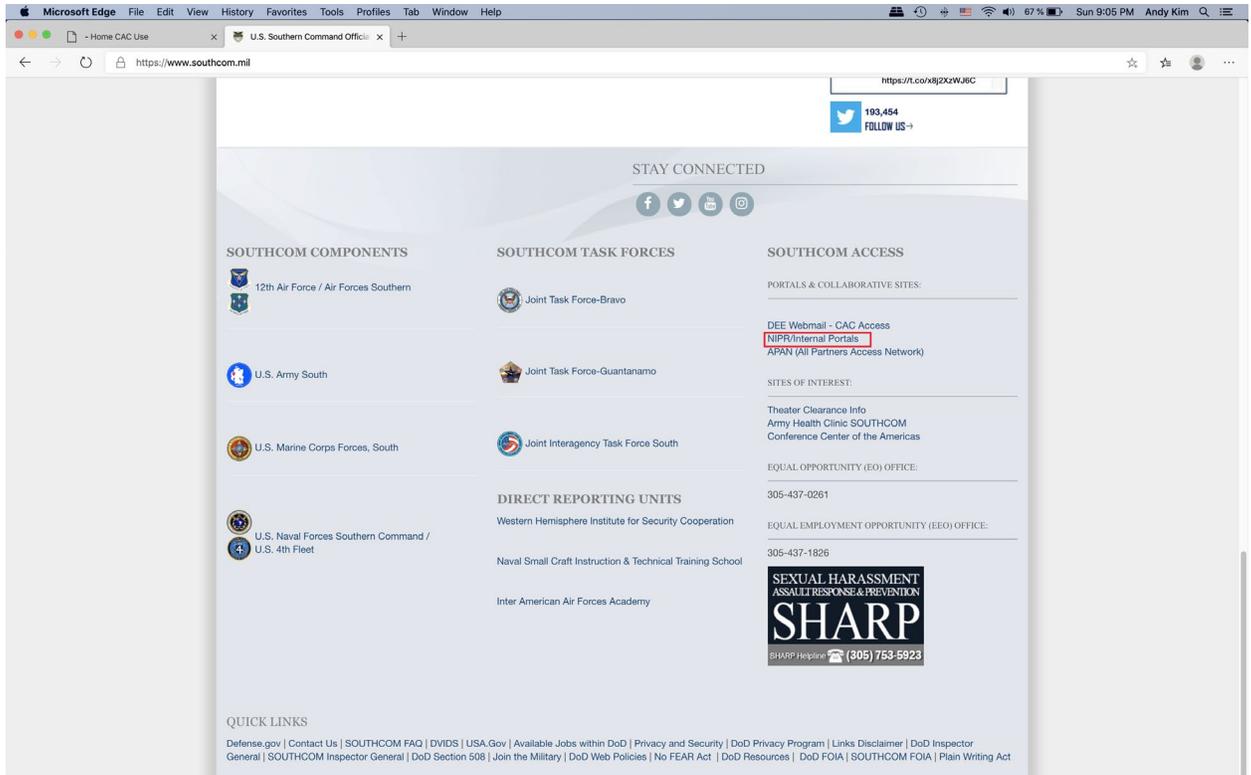
nCSF  
Admiral cell 305 905 5897  
SgtMaj cell 305 812 9326

-----  
SOUTHCOM Colleagues,

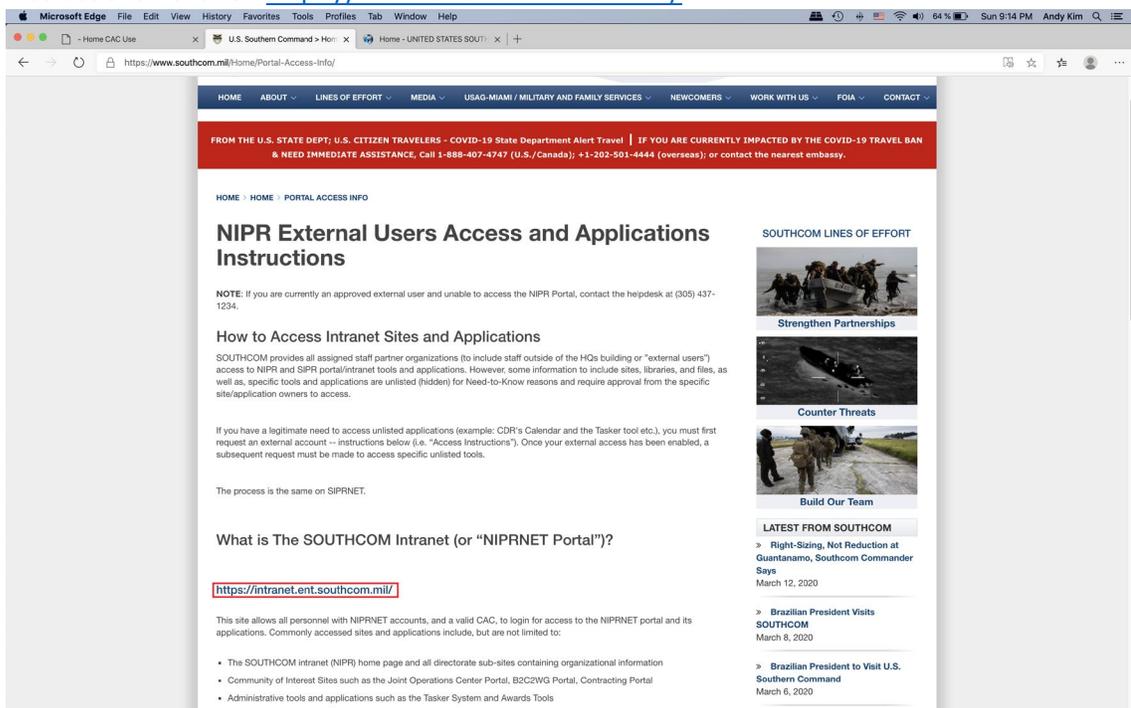
We are in an unprecedented situation with tens of thousands of American citizens around the world who would like to return to the United States due to the COVID19 pandemic. As airports are closed in many countries not allowing commercial flights and borders closed, American citizens are waiting for guidance on how best to get back to the United States. As quarantine measures go into place, American citizens are reaching out to any possible contact

# Instructions for NIPR Portal Access

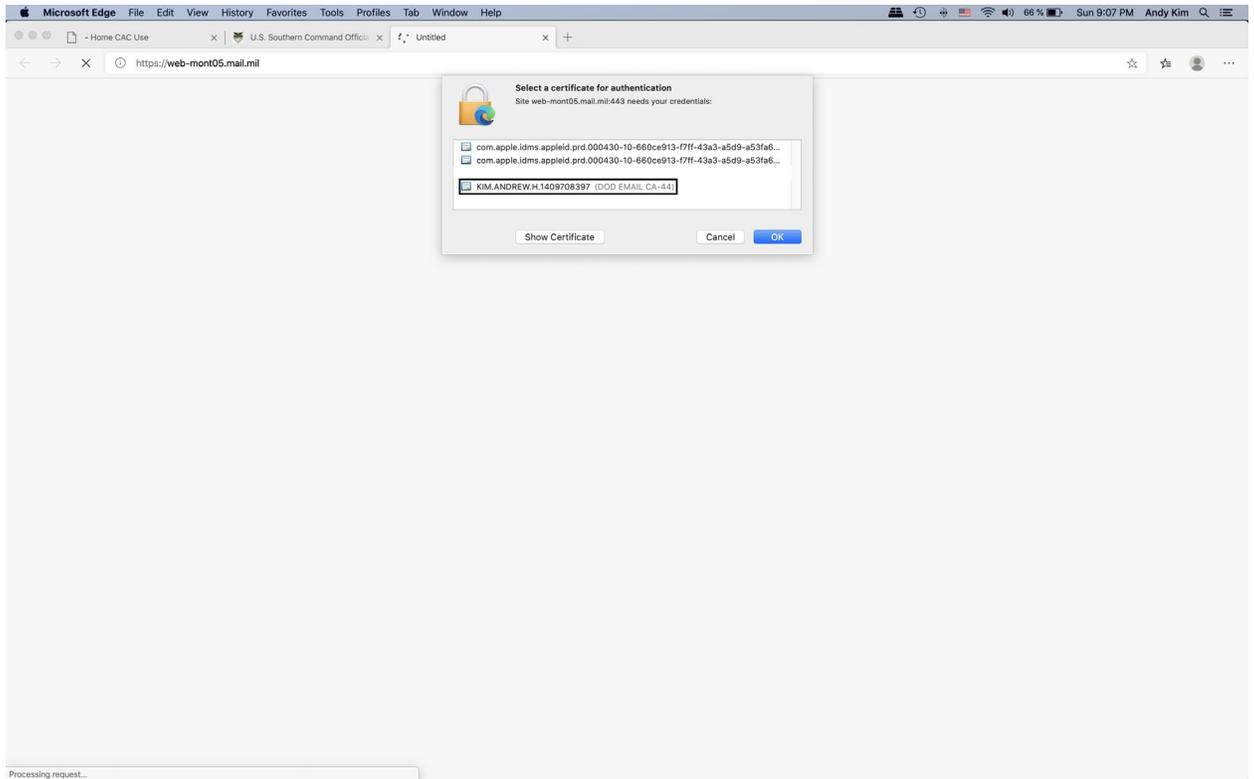
1. Go to URL: <https://www.southcom.mil> and scroll to the bottom until you see NIPR/Internal Portals link and click on the link.



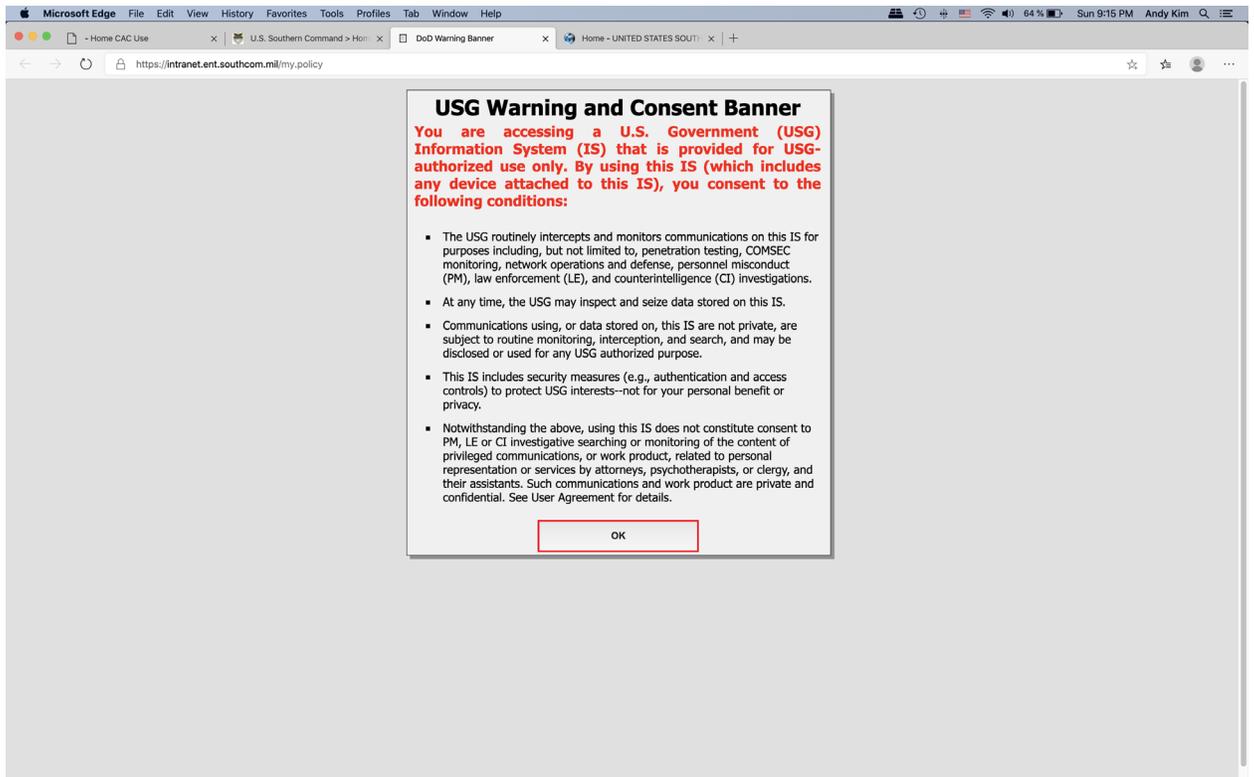
2. You will be taken to another page titled NIPR External Users Access and Applications Instructions. Click on <https://intranet.ent.southcom.mil/>



3. Select (DOD EMAIL CA-44) Certificate.



11. You will now be directed to the DoD Warning Banner, click ok to proceed.



## 12. Enter your PIN.

The screenshot shows a Microsoft Edge browser window with the address bar displaying `https://intranet.ent.southcom.mil/my.policy`. The main content area features a large warning banner with the following text:

**USG Warning and Consent Banner**  
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device connected to the IS for CAC authentication), you acknowledge that the USG may inspect and seize data stored on this IS. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Overlaid on the banner is a smaller dialog box titled "Microsoft Edge" is trying to authenticate user. It contains the text "Enter PIN to allow this." and a PIN input field. Below the input field are "Cancel" and "OK" buttons. A red dashed box highlights the PIN input field and the "OK" button.

## 13. You will now arrive at SOUTHCOM's NIPR Portal.

The screenshot displays the SOUTHCOM NIPR Portal homepage. At the top, there is a navigation bar with the command name "UNITED STATES SOUTHERN COMMAND" and the tagline "PARTNERSHIP FOR THE AMERICAS". A search bar is located on the right side of the header. Below the header, a horizontal menu lists various sections: Home, CMD Group, J1, J2, J3, J4, J5, J6, J7/9, J8, USAG, USANEC, COIs, Help Desk, and Resources. The main content area is divided into several sections:

- Knowledge Wall:** A vertical sidebar on the left with categories like "USSOUTHCOM News", "Command and Special Staff", "Chief of Staff", "Manpower and Personnel", "Intelligence", "Operations", "Logistics", "Strategy, Policy, and Plans", "Communications Systems", "Exercises and Coalition Affairs", and "Resources and Analysis".
- Search:** A search bar with the text "Search ..." and a "GO" button.
- USSOUTHCOM News:** A central section featuring a large blue banner with the text "KEEP CALM AND WASH YOUR HANDS" and a sub-headline "Coronavirus Info for SOUTHCOM Personnel ... Read More". Below the banner are links for "PAO Calendar...", "Latest Articles...", and "Newcomers Portal...".
- Area of Responsibility:** A sidebar on the right containing a list of services and resources: "Announcements", "I need to...", "Tasks & Apps", "Appreciation - Peer to Peer", "Battle Rhythm", "Country Roster-Key Leaders", "Emergency Numbers", "FDMS", "Health of Command", "Insider Threat Program", "IT Self Service Center", and "Job Openings & Training".
- Additional Resources:** On the far right, there are several vertical banners and logos, including "KEEP CALM AND WASH YOUR HANDS", "Daily Muster", "FUOPS OPT (COVID-19)", and "APAN Community".