Cyber Engineering & Digital Transformation (SEA 03)

User Guide
Remote Access & Connectivity Toolkit



March 2020

NAVSEA SEA 03 - Cyber Engineering & Digital Transformation Document Control & Compliance List					
DOC ID#	TYPE	DOCUMENT TITLE	PROCESS OWNERS	VERSION #	RELEASE DATE
S0320-U10-1.1	User Guide	User Guide: Remote Access & Connectivity Toolkit *(Basic)*	• Front Office - CIO & CoS • Policy, Portfolio, Communication, & Competency (P^2C^2)	1.1	3/12/2020
S0320-U11-1.0	User Guide	User Guide: Remote Access & Connectivity Toolkit (*Advanced)*	• Front Office - CIO & CoS • Policy, Portfolio, Communication, & Competency (P^2C^2)	1.0	TBD

Document Disclaimer:

This User Guide ("document") should NOT be construed as legal advice, employment guidance, policy or counsel. The U.S. Department of Navy (DoN), NAVSEA, nor its contributors shall be held liable for any improper or incorrect use of the information provided and/or contained in this disclaimer; and assumes no responsibility for damages associated with or arising from anyone's use of the information in this document.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the Department of Navy , and such reference shall not be used for advertising or product endorsement purposes. For product and vendor references provided in this document, all warranties of any kind, express or implied, including but not limited to the IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, freedom from contamination by computer viruses, spillage, and non-infringement of proprietary rights ARE DISCLAIMED. DON, NAVSEA does not make claim to these such products and they are not to be considered government furnished equipment ("GFE").

Navy personnel and contractors should consult with your authorized leads, designated supervisors and/or duly appointed officers/representatives about their compliance and adherence to applicable laws, policies, responsibilities and statements of work regarding supporting the Department of Navy in a remote capacity ("telework"). This document does not grant authority to ("empower") personnel either in an implied or expressed capacity *to* telework. Any use of this document for such empowerment, in connection to, a derivative of, a supplement to, incorporation of, as a replacement for standing guidance or memos from the DoN regarding telework is strictly prohibited.

Until further amended, the designated Process Owners for this document, are the only parties authorized to make alterations to this document.

Policy Reference:

This User Guide ("document") should NOT be considered or interpreted as legal advice, employment guidance, policy or counsel. All guidance regarding IT policy are provided by the Department of Navy Chief Information Officer (DoN CIO). Personnel are highly encouraged to stay up-to-date on the latest version of DoN CIO's guidance on *Acceptable Use of DoN Information Technology*.

The following link will direct you to the DoN CIO's page for access to Department of the Navy information technology, information management and cybersecurity policy and guidance.

https://www.doncio.navy.mil/Policy.aspx

TABLE OF CONTENTS

For additional support, please reach out to your designated ACIO.

⚓ My ACIO is: _____

1 OVERVIEW

As mandated by the Homeland Security Presidential Directive 12 (HSPD-12), Office of Management and Budget (OMB) M 11-11, and Department of Navy (DON), the Naval Sea Systems Command (NAVSEA) Chief Information Office (OCIO) has deployed hardware, software, and configuration changes that enable the NAVSEA enterprise to log on to their computers and access systems remotely via Navy/Marine Corps Intranet (NMCI).

Government furnished equipment (GFE) is strongly recommended for regular, recurring remote access. Use of GFE guarantees segregation of government information from personal devices and ensures the device meets current DON information assurance standards. Use of GFE also ensures that the appropriate device management controls, such as remote disk wiping, and software, such as antivirus, are present and up-to-date.

The intention of this Remote Access & Connectivity Toolkit (RACT) is to provide you with what IT tools are presently available to you to work remotely. As outlined in the matrix below, this RACT is structured from easiest manner to connect to the more complex manner to connect remotely.

Remote Access & Connectivity Toolkit Complexity Matrix		
COMPLEXITY [Scale 1 to 3]	**RESOURCE**	**REQUIREMENTS/RISKS**
★	**Outlook Web Access (OWA)**	*Internet connection *NMCI Account * Laptop (GFE *or* non-GFE) *Non-NMCI Laptops [will have addt'l steps to follow] * CAC Reader *[can purchase online or work w/ your ACIO]*
★ ★	**Remote Access Service (RAS)**	*Internet connection *NMCI Account * Laptop (GFE) * CAC Reader *[All GFE laptops & devices should have a CAC Reader]*
★★★	**Enhanced Virtual Desktop (EVD)**	*Internet connection *NMCI Account *EVD Account [this is user specific, as this tool gets issued fr. an ACIO. EVD is an addt'l service that has to be ordered] * Laptop (GFE *or* non-GFE) * CAC Reader *[can purchase online or work w/ your ACIO]*
★★★	**MobiKEY**	*Internet connection *NMCI Account * Laptop (GFE or non-GFE) * MobiKEY User Hardware *[this is user specific, as this tool gets issued fr. an ACIO]* **RISK: If the host computer loses power or connectivity the User's connection will be lost*
★★★	**GFE iPhone**	*Data Plan [already provided] *NMCI Account * iPhone (GFE) * Blackberry UEM Account [*this is user specific, as this tool gets issued fr. an ACIO or*

The Chart above is rated on a scale from 1 to 3, with 3 being more complex in nature relative to additional access and/or asset requirements. The ratings will be denoted by "stars". ★

2 Wi-Fi & HOTSPOTS

Most portable devices, such as laptops, smart phones and tablets, come with built-in Wi-Fi wireless capability. NMCI users can now access, without compromising network security, the NMCI network from Wireless Fidelity (Wi-Fi) networks; such as hotspots in hotels, coffee shops, airports, homes and other venues providing wireless Internet access.

⚓ **:** Make sure the Wi-Fi button on your computer is enabled, it should be white.

Public Hot Spots. The only accepted method of connecting to a DoN network via a public hot spot is via a GFE laptop with the proper Designated Accrediting Authority approved Wi-Fi hardware and software installed. The use of a device's native Wi-Fi capability is not allowed.

Home Networks. Use of a home Wi-Fi network to provide the connectivity for telework is allowed. Home networks should be set up in accordance with guidance from the DoN Chief Information Officer and/or the National Security Agency.

Cellular/Mobile Networks. Approved GFE smart phones and tablets, generally connect through a commercial cellular network as the primary link to the network.
U.S. cellular providers are generally considered to provide a secure, encrypted connection that supports remote access. Some foreign cellular networks are considered "unsecure" and should not be used. Consult with your local information assurance manager (IAM) or security officer for up-to-date travel guidance whenever taking a cellular, or any wireless device, outside the continental United States.

⚓ **:** USB tether is **not** permitted with GFE devices, as it will result in an account -and- potential system lockout.

To access a HotSpot from a cellular/ mobile device, following these steps:

On your iPhone:

> **Open Settings** on your iPhone
> **Open Personal Hotspot**
> Select **Allow Others to Join**

Just below this you will have your default Wi-Fi Password (You can use Hotspot with the Wireless instructions)

3 NMCI SUPPORT

For issues with accessing the NMCI network, you should reach out to them ***first*** before contacting your ACIO.

NMCI can reached via the following toll-free phone number: 1-866-843-6624

For additional technical support, the NMCI offers, Training, Support and Services Management via the following website: https://www.homeport.navy.mil/home/

4 OUTLOOK WEB ACCESS (OWA) ★

One of the primary telework products for Web access is Microsoft OWA, which provides a version of desktop email, contacts and a calendar application. Some functionality is lost because access to network drives and other peripherals is not available. At the same time, access to OWA is practically unlimited. Another advantage is that OWA may be used on personally owned equipment with the addition of a smart card reader.

OWA, used in conjunction with Web portals, is the preferred telework solution for personnel whose remote work can be accomplished without access to network-based services, such as a network drive.

⚓: For the ***best*** possible user experience, it is recommended that you use **Internet Explorer 11** as your browser. All of the instructions that follow assume that you are using Internet Explorer 11.

You can access OWA via the following links for each location, select the URL associated to your log-on domain.

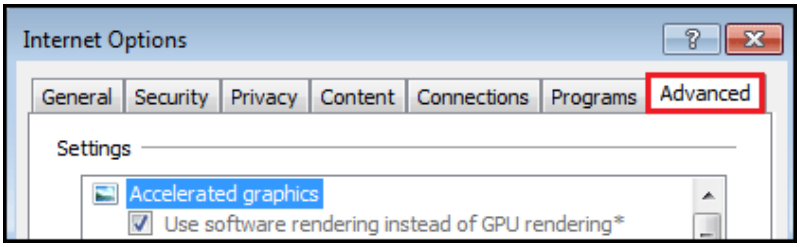
East Coast (NADSUSEA)…
https://webmail.east.nmci.navy.mil/exchange/

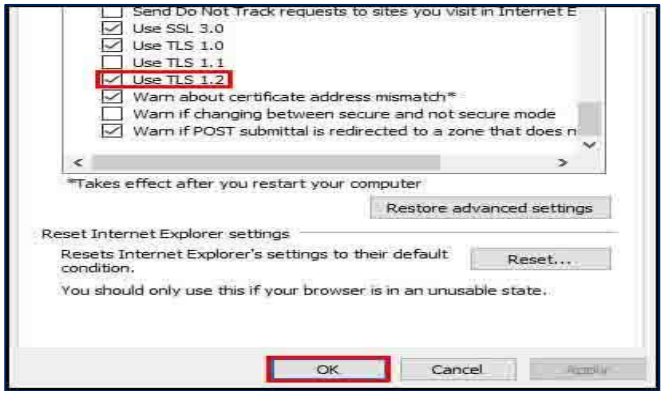
West Coast (NADSUSWE)…
https://webmail.west.nmci.navy.mil/exchange/

⚓: Microsoft Outlook Web Access (OWA) requires that Transport Layer Security (TLS) 1.2 be enabled. Enabling TLS 1.2 secures transmitted data using encryption. This setting is required to access OWA.

The following are step-by-step instructions on how to access OWA:

1. Open Internet Explorer.
2. Click **Tools** | **Internet options**.
3. Click the **Advanced** tab.





4. Under *Security*, select **Use TLS 1.2**
5. Click **OK** to save the settings and close the window.
6. Close and reopen your browser.

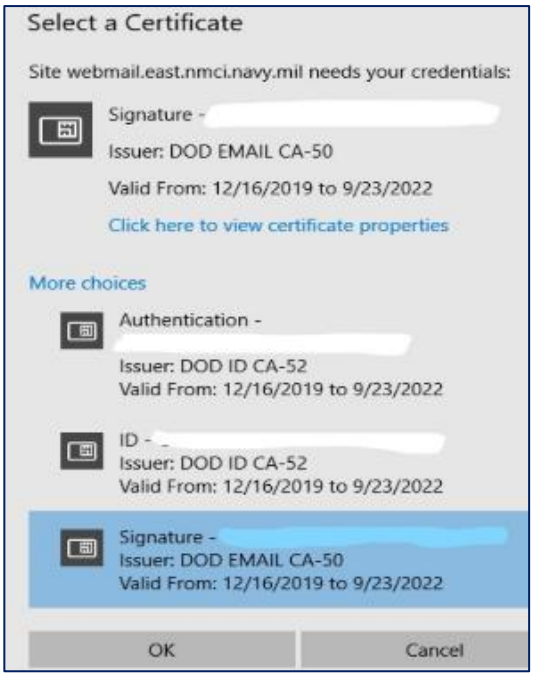
7. Once you access the site, you will be prompted to pick a Certificate.

   Tip: There are 4 types of Certificates: ID, E-mail, PIV and Encryption

8. A Windows Security box will appear. Check to ensure that the name in the Signature field is your name with the correct DOD #. In the **Issuer** field, select the **DOD EMAIL** option, as shown in below in the CORRECT image.

WRONG

CORRECT



⚓ **:** If your certificates do not appear, refer to PKI Certificate Selection Window is Empty or Does Not Appear.

9. If prompted, type your CAC personal identification number (PIN) and click **OK**. Once connected, your mailbox will appear.
   ⚓ **:** First time users will be prompted to select a time zone.

10. When you are finished with OWA, sign out and shutdown the computer. Refer to Sign Out of NMCI OWA
    ⚓ **:** After 15 minutes of inactivity you will be signed out automatically.

For additional training on how to access and use OWA, please following this link:
https://www.homeport.navy.mil/training/OWA

5 REMOTE ACCESS CONNECTION (RAS) ★★

Various options exist for connecting remote devices to DON networks. Teleworkers can access most unclassified Defense Department and DON CAC-enabled websites through the Internet, but some government sites may only be accessed through a VPN connection.

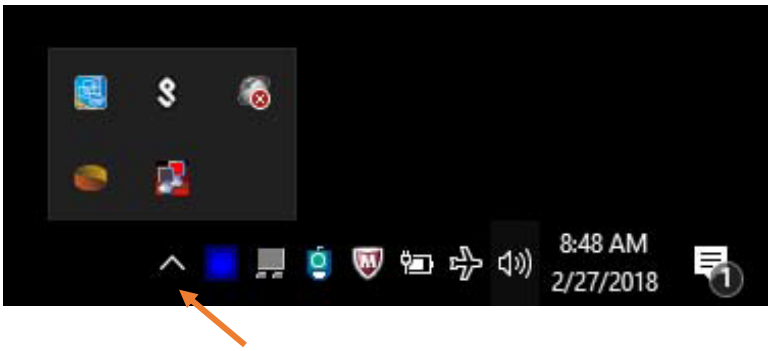
The following are step-by-step instructions on how to access NCMI via RAS over a wireless connection:

On your Desktop navigate to the bottom right corner of the Home Screen near the Time and Date field. You should see the following icon "^".

Once you locate this icon, follow these steps:

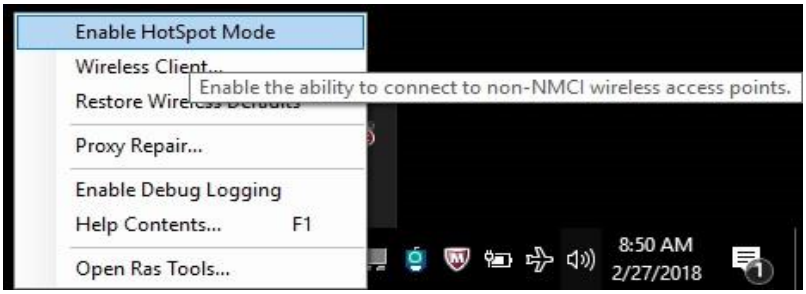
1. Click the ^ next to the status bar to see hidden icons.

Image A- 1

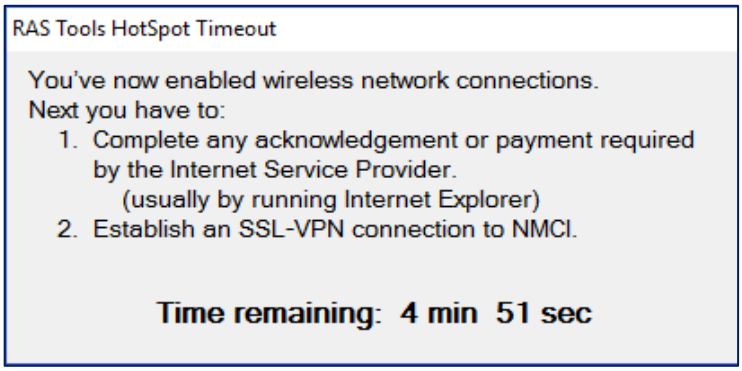


2. Right click the **RAS Tools icon** *(as shown in Image A-1)*

3. Select **Enable HotSpot Mode** from the dropdown selection box



A timer box will appear and begin counting down from 5 minutes. You have 5 minutes to connect to the Wi-Fi connection you will be using, and to open the VPN connection to NMCI.



⚓: If you are having issues connecting to the internet, check your Wi-Fi connection strength. If your signal strength is less than moderate, you might experience slow or no connectivity. Move to an area with moderate or strong signal strength.

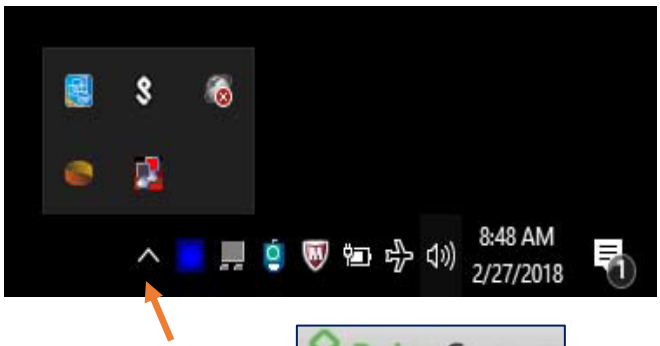
Tip: Browse to a public website such as www.google.com or www.navy.mil to verify you have Internet connectivity.

⚓: If you cannot access a public website, you will need to troubleshoot your Internet connection with the appropriate ISP. If you are in a hotel and get redirected to the hotel's website, follow the hotel's instructions regarding activating your Internet connection.

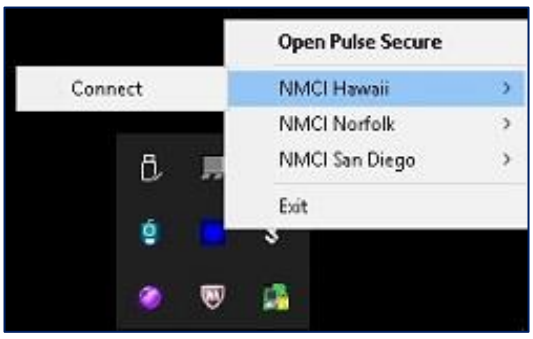
Once you have established the Wi-Fi Connection, continue to these steps:

4. Navigate ***back*** to the bottom right corner of the Home Screen near the Time and Date field. You should see the following icon " ^ " . Click the ^ next to the status bar to see hidden icons

Image A- 1



5. In the task bar, right-click the **Pulse Secure** icon (it looks like an S").



6. In the list that appears, select the closest VPN gateway to your physical geographical location**

(Hawaii, Norfolk or San Diego) and click **Connect**.

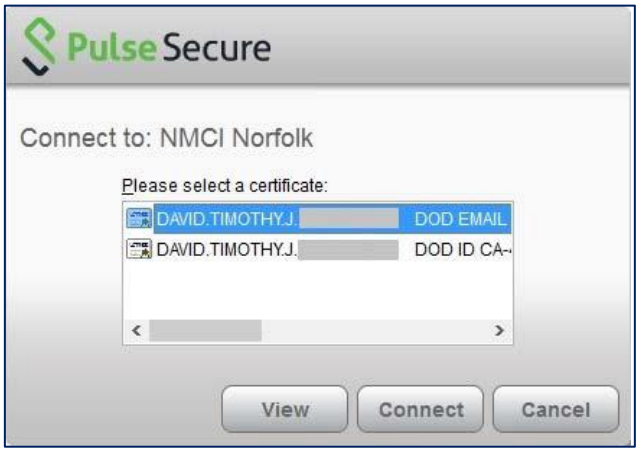
**Tip: Although your main work location is Washington, DC, if you are on travel and teleworking from California, you should select the NMCI San Diego VPN Gateway*

⚓: If there is a problem connecting with one gateway, you can choose an alternate gateway.

7. Select your e-mail certificate in the box that appears and click Connect (*as shown in Image A-2*)

Open the Pulse Secure control panel to verify the connection is established. **Once the VPN connection is established, you can start working normally.**

Image A-2



⚓: With a VPN connection established, the RAS Tools icon will show *NMCI Connected* instead of *Internet Connected*.
If you cannot establish a VPN connection from a Wi-Fi Hotspot, connect a network cable from laptop to a router/home modem.

******The following Tools are additional options for working remotely. As such, acquiring these options shall require approval and coordination with the designated Activity Command Information Office (ACIO) for your Organization. ******

6 ENHANCED VIRTUAL DESKTOP (EVD)★ ★ ★

For more information check out https://www.homeport.navy.mil/support/articles/evd-cfg-essentials

7 MobiKEY ★ ★ ★

The MobiKEY solution allows USN users to control their authorized computers (also called host computer) remotely that are running at a government office or base.

8 GFE iPhone ★ ★ ★

E-mail is accessed through a Blackberry UEM.

9 CAC Readers

A common access card (CAC) is a Unites States Department of Defense (DoD) smart card for multifactor authentication. CACs are issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, non-DoD government employees, state employees of the National Guard and eligible contractor personnel. In addition to its use as an ID card, a CAC is required for access to government buildings and computer networks.

Websites Accessible Through CAC Reader Using an NMCI Computer (Without VPN*)		
WEBSITE NAME	**URL**	**PURPOSE**
DADMS & DITPR-DON	https://www.dadms.navy.mil/	IT Portfolio Management
CAS2NET	https://cas2net.army.mil/	Fill out mid-year assessment
Defense Travel System (DTS)	https://dtsproweb.defensetravel.osd.mil/dts-app/pubsite/all/view/	Book official travel and manage travel expenses
E-Drug	https://www.edrugtest.com/	Use for drug testing purposes
eMASS	https://navy.emass.apps.mil/	Supports mission information assurance analysis
EDW Trackers	https://edw.csd.disa.mil/	Pull metrics and data Submit SF-182s
iNAVSEA	https://navsea.navy.deps.mil/Pages/default.aspx	Access to internal NAVSEA pages and
LinkedIn Learning	www.linkedin.com/learning/ (login with Navy email, add activate at end of link if not registered)	Complete courses for professional and personal development
MILCONNECT	https://milconnect.dmdc.osd.mil/milconnect/	Manage employee benefits and records
NAV-ITAS	https://navitas.navy.mil/	Navy Information Technology Purchase Requests (ITPR)
Navy e-Learning	https://learning.nel.navy.mil/ELIAASv2p/	Complete various mandatory training (telework, etc.)
NAVSEA eTools	https://navseahq.navy.mil/tracker/navseaetools/launch	Access ART, eTAT, ePRD, contractor property pass Request DON Tracker license
Navy Family Accountability and Assessment System (NFAAS)	https://navyfamily.navy.mil/	Accounts, assesses, manages, and monitors the recovery process for personnel and their families affected and/or scattered by a wide-spread catastrophic even
Navy Knowledge Online (NKO)	https://my.navy.mil/	Hosts some mandatory trainings
TWMS	https://twms.navy.mil/login.asp	Complete mandatory training Review personnel information Check in new employees Pull PRD numbers Access supervisory hierarchy
USA Staffing (Onboarding Manager)	https://usastaffing.gov/	Review Certs and applicant qualifications Track hiring action status, onboarding document submissions, security clearances, etc. Send official offers

⚓: All of the above sites were tested offsite 11 March 2020. If you are unable to access, contact your ACIO for support

10 VPN Accessibility

A VPN provides a secure, encrypted connection to a network from an outside location, normally through the use of a laptop, but also through other devices. A VPN-connected laptop can provide the full range of network functionality that users would experience from their desktop in the office. VPN access can be accomplished through a wired connection, a cellular air card or an approved Wi-Fi connection. However, the number of VPN ports on the network is limited.

Notable Websites Inaccessible Without VPN		
DCPDS (MyBiz+/HR Application)	https://compo.dcpds.cpms.osd.mil/	Update supervisor information Submit RPAs Pull 50s
EDW Trackers	https://edw.csd.disa.mil/	Pull metrics and data Submit SF-182s
ERP	https://ep.erp.navy.mil/irj/portal	Manage time/attendance, training requests, IDP
FAS CLASS	https://ACPOL2.ARMY.MIL/FASCLASS	Search PDs and organizational information
HR Link	https://hrlink.donhr.navy.mil/	Pull standard reports from DCPDS
OCHR Partner Portal	https://portal.secnav.navy.mil/my.policy	OCHR version of iNAVSEA (SharePoint)
PBIS-IT	https://fmbweb1.nmci.navy.mil/cfdocs/pbisit/index.cfm	IT budget tracking tool
WNY-FM Portal	https://wnyfm.nmci.navy.mil/portal/	Use for TIES and search asset information

⚓: All of the above sites were tested offsite 11 March 2020

APPENDIX A
Call Forwarding & Voicemail

Cisco IP phone and Unity Voice Mail
Model # 8841 & 8851

Forward All Calls

⚓ : To forward all incoming calls to another number:

- Press the **CFwdALL** soft key. You hear a confirmation beep.
- Dial the number to which you want to forward all your calls. Dial the number exactly as if you were placing a call to that number. Remember to include locally required prefix numbers.
- The phone display is updated to show that calls will be forwarded.
- Press the pound key **(#) or the EndCall** soft key**.**

⚓ : To forward calls to voice mail

- Manually enter the voice mail number, -or- use the
- **CFwdALL** soft key plus the **Messages** button, followed by the **EndCall** soft key.
- When call forward all is set, the display shows the Call Forward Icon.

⚓ : To forward calls to a speed-dial number

- Press the **CFwdALL** soft key plus a **speed-dial button**, followed by the **EndCall** soft key.

How To Access Voicemail

⚓ : To access voice mail externally

- Dial (202) 781-1111
- At the first prompt enter your 5 digit extension (e.g. 1-2345) and #. At the second prompt enter in your voice mail pin. This is the same pin used when accessing messages internally

To cancel call forwarding:

• Press the **CFwdALL** soft key.

Cisco IP phone and Unity Voice Mail
Model # 7962 & 7965

Forward All Calls

⚓ : To forward all incoming calls to another number:

- Press the **CFwdALL** soft key. You hear a confirmation beep.
- Dial the number to which you want to forward all your calls. Dial the number exactly as if you were placing a call to that number. Remember to include locally required prefix numbers.
- The phone display is updated to show that calls will be forwarded.
- Press the pound key **(#) or the EndCall** soft key.

⚓ : To forward calls to voice mail

- Manually enter the voice mail number, -or- use the
- **CFwdALL** soft key plus the **Messages** button, followed by the **EndCall** soft key.
- When call forward all is set, the display shows the Call Forward Icon.

⚓: To forward calls to a speed-dial number

- Press the **CFwdALL** soft key plus a **speed-dial button**, followed by the **EndCall** soft key.

How To Access Voicemail

⚓: To access voice mail externally

- Dial (202) 781-1111
- At the first prompt enter your 5 digit extension (e.g. 1-2345) and #. At the second prompt enter in your voice mail pin. This is the same pin used when accessing messages internally

To cancel call forwarding:

• Press the **CFwdALL** soft key.

APPENDIX B
Best Practices

- Make sure you have a power supply that fits your NMCI computer
- Download needed documents ahead of time to your desktop
- Verify your Property Pass and make sure it has not expired. Contact your ACIO if you need assistance
- Have an external CAC reader handy. Contact your ACIO if you need assistance
- Ensure you have a CAC reader, if you plan to take your workstation keyboard home (to use the CAC reader), remember to bring your keyboard back to the office when you return. If you need a loaner contact your ACIO
- Make sure the Wi-Fi button on your computer is enabled, it should be white
- If you experience problems connecting remotely, navigate to **"Start,"** scroll to and click "**Configure Enterprise Wireless Profile**"
- One of the most commonly missed steps using RAS Tools is making sure "**HotSpot Mode"** is enabled
- Remember not to connect hardware aside from a mouse, keyboard, and or monitor to the USB port on your NMCI computer
- Do not connect a wireless printer to your NMCI computer when working remotely
- Naval Nuclear Propulsion Information (NNPI) access requires VPN
- Work during off-cycle hours.
  For example, network saturation peeks during the hours of 0800 – 1700
- Use remote access to connect, download email; then work offline
- Connect your NMCI computer directly to the RJ45 port https://en.wikipedia.org/wiki/Registered_jack on your router using an Ethernet cable, for example, see the following link: https://en.wikipedia.org/wiki/Ethernet#/media/File:Ethernet_Connection.jpg
- Remember to disable "**HotSpot Mode"** when you return to the office