

USER RESPONSIBILITIES

A Support Tracking System (STS) ticket **MUST** be submitted for ALL IT Support, Hardware and Software requests. Submit a ticket online at:

<https://apps.navfac.navy.mil/pls/apex/f?p=198:3>

- Keep your passwords protected
- Keep your accounts (i.e. Portal, TWMS, SIPR-NET, etc.) up-to-date by logging in every 29 days **NOTE: NMCI and official DoD/DoN websites will disable accounts after 30 days and delete accounts after 45 days of inactivity**
- Manage your computer files by deleting unwanted files and archiving needed files
- Do not use network drives to ARCHIVE data
- Back up your data
- Track the location of the files you place on the network shared drives
- Secure all Privacy Act, personal, and Controlled Unclassified Information (CUI) and encrypt email when sending
- Notify CIO2 immediately if any cybersecurity incident occurs (i.e. viruses, classified/sensitive data spillages, network attacks) via email NAVFACSW_CIO2@us.navy.mil
- Notify the Command Security Officer navfac_sw_security_ud@us.navy.mil of unauthorized disclosure of privacy act, personal, and CUI
- Complete **annual** Cyber Awareness Challenge training
- Ensure your supervisor provides a list of email distribution lists you need
- Manage your email inbox
- Update your employee information in ID Card Office Online <https://idco.dmdc.osd.mil/idco>
- Do not leave your CAC in your computer when you walk away

CIO1-INFORMATION SYSTEMS (IS)

- Business Systems/Enterprise Application access provisioning and troubleshooting
- Public and private portal management (AFPIMS, SharePoint Online)
- Enterprise/Cloud application development
- Application configuration and database support

CIO2—CYBERSECURITY (CS)

- Cybersecurity Incident Response for IT and OT (i.e. viruses, spillages, email & network attacks)
- SAAR Processing for Network & System Accounts
- Cybersecurity Workforce Program Management
- Cybersecurity support for Projects and Contracts
- Risk Management Framework sustainment
- Requests for FRCS Authority-to-Operate (ATO)

CIO3-INFORMATION TECHNOLOGY (IT)

- NMCI Ordering and Account Management
- Workstation Hardware and Software Support
- VTCs, Desk & Mobile phones, tablets, etc.
- File Share Access (Network Folders) & Storage
- Inventory (Laptops, Hard Drives, Printers, etc.)

Training Videos & Self Help Links:

https://flankspeed.sharepoint-mil.us/sites/navfac_sw_command_information_office/sitepages/cio3-it.aspx

CIO4-OPERATIONAL TECHNOLOGY (OT)

- Smart Grid/Energy
- SCADAs, DDCs, HVACs
- Utility Control Systems (UCS)
- Building Control Systems (BCS)
- Advance Metering Infrastructure (AMI)
- Cybersecurity for Industrial Control Systems

CIOR-RESOURCES MANAGEMENT

- IT Procurements
- Community Management
- Budget Development and Execution

IMPORTANT LINKS

Flank Speed Hub

https://flankspeed.sharepoint-mil.us/sites/flank_speed_hub

NAVFAC CIO Support Tracking System (STS)

<https://apps.navfac.navy.mil/pls/apex/f?p=198:3>

DON CIO Acceptable Use Policy

<https://www.doncio.navy.mil/filehandler.ashx?id=15341>

NMCI Enterprise Self-Service Portal

<https://servman/sm/ess.do>

NAVFAC Southwest CIO SharePoint

[https://flankspeed.sharepoint-mil.us/sites/NAVFAC_SW_Command_Information_Office/SitePages/Command-Information-Office-\(CIO\).aspx](https://flankspeed.sharepoint-mil.us/sites/NAVFAC_SW_Command_Information_Office/SitePages/Command-Information-Office-(CIO).aspx)

ID Office Online - Global Address List (GAL) Updates

<https://idco.dmdc.osd.mil/idco>

Locate Your NAVFAC SW ACTR

https://flankspeed.sharepoint-mil.us/sites/navfac_sw_command_information_office/sitepages/cio3-it.aspx

SAAR Sample and Resources

https://flankspeed.sharepoint-mil.us/sites/NAVFAC_SW_Command_Information_Office/SitePages/SW-SAARN-Instructions.aspx

How To Obtain NMCI Account

https://flankspeed.sharepoint-mil.us/sites/NAVFAC_SW_Command_Information_Office/SitePages/obtain-new.aspx

Gain Contractors in TWMS

https://flankspeed.sharepoint-mil.us/sites/NAVFAC_SW_Command_Information_Office/SitePages/gaining-ktrs-in-twms.aspx

ieFACMAN - <https://iefacman.navfac.navy.mil>

MAXIMO - <https://maximo.navfac.navy.mil>

DoD Safe - <https://safe.apps.mil>

NMCI Homeport - <https://homeport.navy.mil>

SLDCADA - <https://www.sldcada.dc3n.navy.mil>



COMMAND INFORMATION OFFICE QUICK REFERENCE GUIDE



MAILING ADDRESS

NAVFAC SOUTHWEST, CIO
750 PACIFIC HWY
SAN DIEGO, CA 92132

NMCI SERVICE DESK

COMM: 1-866-843-6624

eMail: servicedesk_navy@nmci-isf.com

NMCI@flankspeed.onmicrosoft.us

WEB: <https://homeport/home/>

NITC 24 HOUR OPS WATCH

DSN: 312-551-2555

COMM: 805-982-2555

NAVFAC SW SUPPORT DESK

COMM: 1-619-705-6161



WHEN IT SERVICES & SUPPORT OPTIONS ARE REQUIRED

IT services and support are available through many different avenues—the NMCI Service Desk, NAVFAC Southwest CIO department, NAVFAC portal Support Tracking System (STS) and NAVFAC Information Technology Center (NITC).

When to Contact NMCI Service Desk

Problems with NMCI owned hardware (Desktops, Laptops, Monitors, Printers, etc.); Restore requests for deleted network files; Computer error messages not associated with NAVFAC applications; Problems with NMCI Image Software (MS Office Suite, WEB browsers, etc.); Network connectivity; Pulse Secure (VPN); website access; Data at Rest (Bitlocker); CAC certificates; computer accounts; computer login problems; and Email issues not specifically covered by NAVFAC CIO.

When to Contact NAVFAC SW CIO

Enterprise Applications (Maximo, HAZWaste, etc.); Network file/folder security administration; NMCI Move-Add-Change (MAC) Requests—i.e. physical relocations and software changes; NMCI/ACTR issue escalation; Telecommunications (i.e. Phones (Desk/Cell), VTC and TELCOMs); Email configuration, distribution lists, public folder creation and folder security; IT Equipment checkout; IT Purchasing; Cybersecurity Incidents; AMI Support and Cyber Security for Industrial Control Systems.

When to Use Support Tracking System

Use STS to request ALL IT hardware, software and services that are not directly supported by NMCI.

WHEN YOU NEED FRCS/OT CYBERSECURITY SUPPORT FOLLOW THE WORK INDUCTION PROCESS

Details Coming Soon!

In the interim, email Nailah Williams,
Nailah.Williams.civ@navy.mil for assistance.

Seat Assignment /Relocation Requests

CIO requests a minimum of 30 days' notice for any personnel movements that require relocation of a NMCI seat. Office renovations that require new cabling will require 45—60 days' notice depending on the extent of re-cabling. **ACTR requires an STS for assistance for this move or requests for seat to ensure CIO inventory is correct.**

Establish an NMCI PIN

IMPORTANT: Your NMCI pin is required for authentication by phone with NMCI. Safe guard and do not share. To update or create your PIN and Secret Word: **1)** Navigate to: <https://servman/sm/ess.do> **2)** Select 'Authentication Information' **3)** Select your name **4)** Enter an Authentication PIN and Secret Word. **5)** Click 'OK' to save



When to Contact NITC 24 Hour OPS Watch DSN: 312-551-2555

Problems with the NAVFAC portal or portal accounts; issues with connectivity to NITC hosted applications; and NITC account password resets.

When to Use the IT Procurement Request

The IT Procurement Request (ITPR) form must be submitted for ALL purchases related to IT hardware, software or services. This includes desktop and cell phones, copiers, faxes, printers, plotters, computer equipment, website hosting and software. ITPRs must be signed by the NAVFAC SW CIO and escalated to NAVFACHQs CIO for final approval. ITPRs are submitted via the Navy Information Technology Approval System (NAV-ITAS).

When to Contact the Command ISSM

Spillages of classified/sensitive data, virus attacks, suspicious email activity, SAAR and RMF support.

When to Request New Employee Account and IT Assets

A new employee's supervisor, management assistant or command sponsor must submit an Employee Check-in ticket via STS to request the creation of a new user account, reset desk phone mailbox and IT Assets (i.e. laptop, keyboard, mouse, external hard drive). A SAAR and current FY Cyber Awareness training certificate are required. SAAR must be submitted via TWMS; if not received, account is subject to being restricted or disabled. New NMCI accounts can be created up to 10 days before the employee comes on-board.

Note: CACs are issued at PSD.