




## Command Information Officer (CIO) Brief for New Employee Onboard

**NAVFAC HAWAII CIO Department**


Updated: 20 Nov 2020



## AGENDA


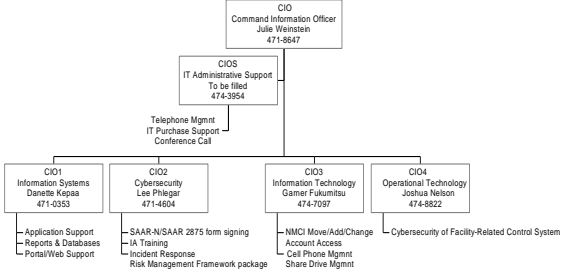


- Command Information Officer (CIO) Organization
- Common Systems
- Initial IT Provisioning
- NMCI & Access Awareness
- User Agreement (part of the SAAR-N form)
- Use of Government Communication Systems
- Common Not-to-Do



2 NAVFAC HI CIO

## NAVFAC Hawaii CIO





```


graph TD
    CIO[CIO  
Command Information Officer  
Jude Weinstein  
471-8647]
    CIO --- CIO5[IT Administrative Support  
To be filled  
474-3954]
    CIO --- CIO1[CIO1  
Information Systems  
Danete Kepaa  
471-0353]
    CIO --- CIO2[CIO2  
Cybersecurity  
Lee Philegar  
471-4604]
    CIO --- CIO3[CIO3  
Information Technology  
Gamer Fukumitsu  
474-7097]
    CIO --- CIO4[CIO4  
Operational Technology  
Joshua Nelson  
474-8822]
    
    CIO5 --- Tel[Telephone Mgmt]
    CIO5 --- Pur[IT Purchase Support]
    CIO5 --- Conf[Conference Call]
    
    CIO1 --- App[Application Support]
    CIO1 --- Rep[Reports & Databases]
    CIO1 --- Port[Portal/Web Support]
    
    CIO2 --- SAAR[SAAR-NSAAR 2875 form signing]
    CIO2 --- IA[IA Training]
    CIO2 --- IR[Incident Response]
    CIO2 --- RM[Risk Management Framework package]
    
    CIO3 --- NMCI[NMCI Move/Add/Change  
Account Access]
    CIO3 --- CP[Call Phone Mgmt]
    CIO3 --- SD[Share Drive Mgmt]
    
    CIO4 --- CF[Cybersecurity of Facility-Related Control System]
    
```

3 NAVFAC HI CIO

## Common Systems




- Navy Marine Corp Intranet (NMCI) is the network.
- NAVFAC Hawaii Web Portal is the intranet.
- Standard Labor Data Collection and Distribution Application (SLDCADA) is for Timekeeping.
- Total Workforce Management Services (TWMS) is for tracking employee information, such as training, clearance, education.
- Support Tracking System (STS) is for requesting IT support.




4 NAVFAC HI CIO

## Initial IT Provisioning




- Your CIO Liaison and/or Supervisor will assist you with:
  - Obtaining your CAC
  - Obtaining your NMCI Computer Account
  - Taking Cyber Awareness Challenge Training
  - Completing a Systems Access Authorization Request - Navy (SAAR-N) in TWMS
  - Obtaining access to share drive(s) business systems and applications:




7 NAVFAC HI CIO

## Install CIO Support Tool

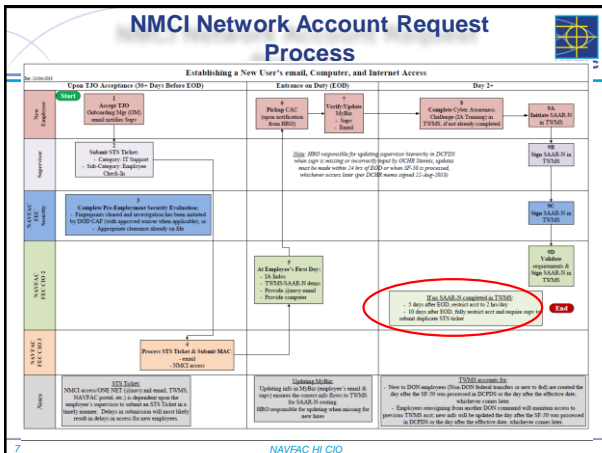


### How to Install CIO Support Tool


1. Copy this link:  
`\\nadsuswe.nads.navy.mil\DFS_NAVFAC_01$\NAVFACHL_BVApps\CIO_SUPPORT_TOOL\dist\install_supporttool.bat`
2. Press the Windows Logo Key + R
3. Paste the copied link above into the text box, and press the ENTER key.
4. A shortcut named "CIO Support Tool" should now be on your desktop.
5. Click on the shortcut to use the tool.




8 NAVFAC HI CIO



## NAVFAC Web Portal



[https://www.navfac.navy.mil/navfac\\_worldwide/pacific/fecs/hawaii.html](https://www.navfac.navy.mil/navfac_worldwide/pacific/fecs/hawaii.html)



8 NAVFAC HI CIO

## NAVFAC Web Portal (Cont.)



<https://hub.navfac.navy.mil/>



9

NAVFAC HI CIO

## NAVFAC HI CIO SUPPORT submit an STS ticket through this site



<https://hub.navfac.navy.mil/webcenter/portal/hi/Support+Lines/Command+Information+Office/CIO+HI+IT+Support>



10

NAVFAC HI CIO

## Computer Accommodation Program



• Computer Accommodation Program can help employees with special needs:

- Blind / Low Vision
- Communication
- Deaf / Hard of Hearing
- Dexterity
- Anything else.

• The website address is: [www.cap.mil](http://www.cap.mil)

11

NAVFAC HI CIO

## NMCI & Access Awareness



• NMCI Help Desk

- NMCI account/login, hardware problems, MS Office, printing issues
- Call 1-866-843-6624, Submit online request, or Email

• Data Backup

- NMCI does not backup the data on your computer.
- Recommend backing up critical data to H: (Home) drive.

• NAVFAC Single Sign On (SSO) Account

- [sso.navfac.navy.mil/register/registration\\_form.jsp](http://sso.navfac.navy.mil/register/registration_form.jsp)
- Register for account to access NAVFAC portal applications.

• Check with supervisor for Enterprise applications & access

- e.g. STS, MAXIMO, ieFACMAN, SLDCADA, share drives

12

NAVFAC HI CIO

## NAVFAC Single Sign On (SSO) Account

[sso.navfac.navy.mil/register/registration\\_form.jsp](https://sso.navfac.navy.mil/register/registration_form.jsp)

13 NAVFAC HI CIO

## User Agreement - Part I

**\*\*EXPECT NO PRIVACY\*\***

**22. USER AGREEMENT - STANDARD MANDATORY NOTICE AND CONSENT PROVISION:**

**By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information system:**

- You are accessing a U.S. Government (USG) information system (IS) which includes any device attached to this information system that is provided for U.S. Government authorized use only.

**You consent to the following conditions:**

- The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE) and counterintelligence (CI) investigations.
- At any time, the U.S. Government may inspect and seize data stored on this information system.
- Communications used, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government authorized purpose.
- This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests—not for your personal benefit or privacy.
- Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigation searching or monitoring of the content of privileged communications or data (including work product) that are related to personnel representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below.
- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operations, protection, or defense, or for communications security. This includes all communications and data on any information system, regardless of any applicable privilege or confidentiality.
- The user consents to interception and review of all communications and data for any authorized purpose (including personnel representation, law enforcement, or counterintelligence investigations). However, consent to interception and review of communications and data is not consent to the use of privileged communications or data for personnel representation, law enforcement, or counterintelligence investigations against the user and does not create an absolute privilege or confidentiality that otherwise applies.
- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek legal counsel on such matters prior to using an information system if the user intends to rely on the protection of a privilege or confidentiality.
- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where those users have established legal standards and DoD policy.
- As with other U.S. Government devices, to identify such communications or data as privileged or confidential does not waive the privilege of confidentiality if such protection otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable steps to identify such communications or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of unclassified privileged communications and data, to ensure they are appropriately protected.
- In cases where the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigations searching, i.e., for all communications and data other than privileged communications or data that are related to personnel representation or services by attorneys, psychotherapists, or clergy, and their assistants, the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise authorized use or disclosure of such information.
- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent banner or notice or other information, or whether the banner banner is visible to the user. The banner banner is visible to the user, regardless of whether the banner banner is visible to the user. The banner banner is visible to the user, regardless of whether the banner banner is visible to the user.

14 NAVFAC HI CIO

## User Agreement - Part II

**USER RESPONSIBILITIES:**

I understand that to ensure the confidentiality, integrity, availability, and security of Navy Information Technology (IT) resources and information, when using those resources, I shall:

- Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or misuse.
- Protect Controlled Unclassified Information (CUI), to include Personally Identifiable Information (PII), and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- Protect authenticators (e.g., Password and Personal Identification Numbers (PIN)) required for login authentication at the same classification as the highest classification of the information accessed.
- Protect authentication tokens (e.g., Common Access Card (CAC), Alternate Logon Token (ALT), Personal Identity Verification (PIV), National Security Systems (NSS) tokens, etc.) at all times. Authentication tokens shall not be left unattended at any time unless properly secured.
- Protect authenticators (e.g., Password and Personal Identification Numbers (PIN)) required for login authentication at the same classification as the highest classification of the information accessed.
- Report all security incidents including PII breaches immediately in accordance with applicable procedures.
- Access only that data, control information, software, hardware, and firmware for which I am authorized access by the cognizant Department of the Navy (DON) Commanding Officer, and have a need-to-know, have the appropriate security clearance. Assume only those roles and privileges for which I am authorized.
- Observe all policies and procedures governing the secure operation and authorized use of a Navy information system.
- Digitally sign and encrypt e-mail in accordance with current policies.
- Employ sound operations security measures in accordance with DOD, DON, service and command directives.

### THINGS YOU MUST DO!

15 NAVFAC HI CIO

## User Agreement - Part III


I further understand that, when using Navy IT resources, I shall not:

- Auto-forward any e-mail from a Navy account to commercial e-mail account (e.g., com).
- Bypass, stress, or test IA or Computer Network Defense (CND) mechanisms (e.g., Firewalls, Content Filters, Proxy Servers, Anti-Virus Programs).
- Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource.
- Relocate or change equipment or the network connectivity of equipment without authorization from the Local IA Authority (i.e., person responsible for the overall implementation of IA at the command level).
- Use personally owned hardware, software, shareware, or public domain software without written authorization from the Local IA Authority.
- Upload/download executable files (e.g., exe, com, vbs, or bat) onto Navy IT resources without the written approval of the Local IA Authority.
- Participate in or contribute to any activity resulting in a disruption or denial of service.
- Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code.
- Use Navy IT resources in a way that would reflect adversely on the Navy. Such uses include pornography, chain letters, unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use, violation of statute or regulation, inappropriately handled classified information and PII, and other uses that are incompatible with public service.
- Place data onto Navy IT resources possessing insufficient security controls to protect that data at the required classification (e.g., Secret, not Unclassified).

### THINGS YOU MUST NOT DO!

16 NAVFAC HI CIO



## Use of Government Communication Systems



**What are Government Communication Systems?**

- Email
- Internet
- Telephones
- Fax machines
- Digital Senders
- Cell phones
- Multi-Function Devices

**For official use and authorized purposes only**



At Virtual orientation briefings/on-boarding, the Naval Facilities Engineering System Command, Hawaii/CIO division provides notification to users of DoD telecommunications and information systems that discussion or transmission of classified information on non-secure systems and/or devices is prohibited. For authorized purposes, these systems are subject to monitoring and usage constitutes consent to monitoring.

17 NAVAFAC HI CIO Nov-20

## Authorized Personal Communications




Authorized "personal communications" from office can be made as long as they:

- Don't adversely affect official duties
- Are of "reasonable" duration & frequency
- Don't overburden the communication system
- Create no significant additional cost to DoD



18 NAVAFAC HI CIO Nov-20

## Common Not-To-Do




- DO NOT Plug USB thumb drive into your work computer.
- DO NOT Charge your phone from your work computer.
- DO NOT Visit unauthorized websites (e.g., pornography or gaming).
- DO NOT Download unauthorized software (e.g., virus or worm).

**ALL of the above will trigger NMCI to restrict logon hours on your account.**

**What to look for:**

- Is the email from a legitimate sender?
- Is the website link from a legitimate source?
- Does my action violate the user agreement?



19 NAVAFAC HI CIO