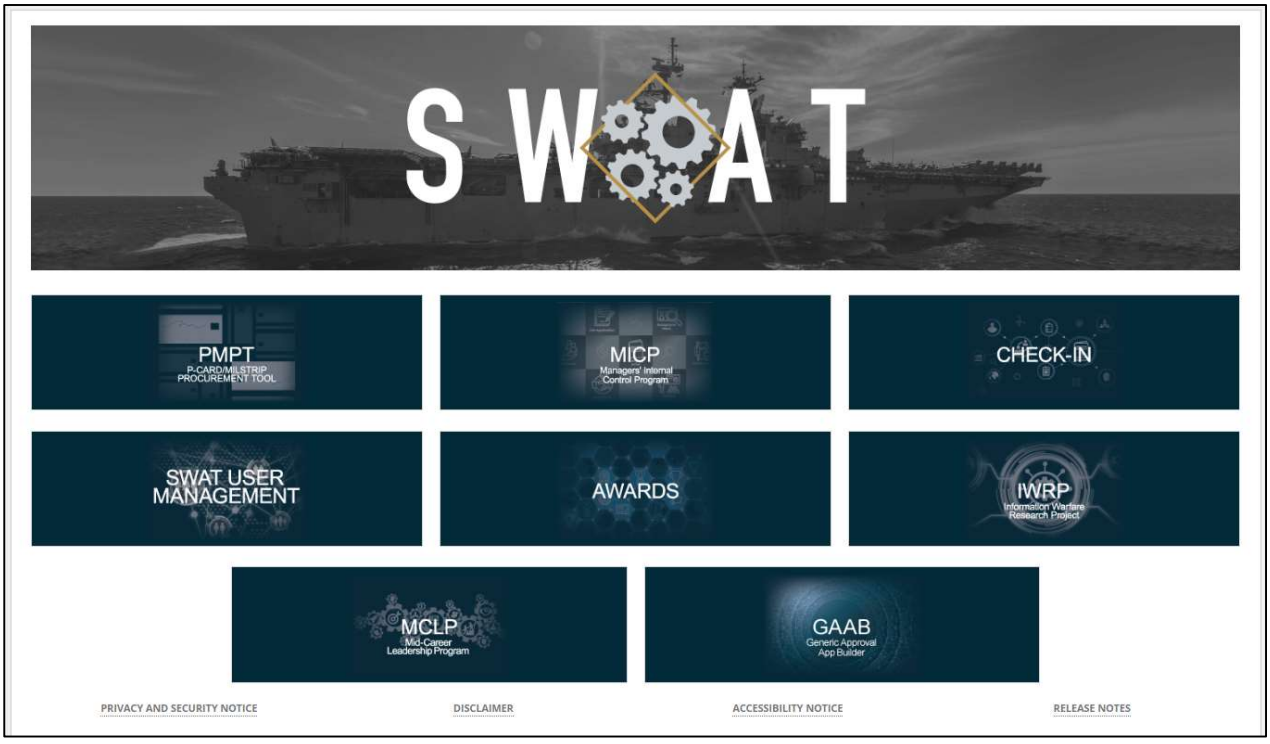
New User Access Instructions for SWAT Check-In:

Step 1: Please go to https://swat.dc3n.navy.mil/suite/sites/niwc-home to verify you have access. ***Users must use their CAC (PIV certificate required) to access the SWAT tool. If you do not have a CAC:*** *you must have a company representative with a SWAT Account or your COR submit a single Check-In Request on your behalf for the following: SAAR-N, CAC, LDAP Account, and NMCI Email. Please attach a valid SAAR-N and Information Assurance (IA) Training Certificate.*

If you have a CAC and you have attempted to access the link above, proceed to either STEP A OR STEP B depending on your **result** below:

Result A: IF you are able to access the following screen, proceed to STEP A:



STEP A: Please select the SWAT User Management application to request access to the Check-In group(s) that you need (see the Check-In Role Key at the end of this document for guidance).

From the SWAT User Management Application:

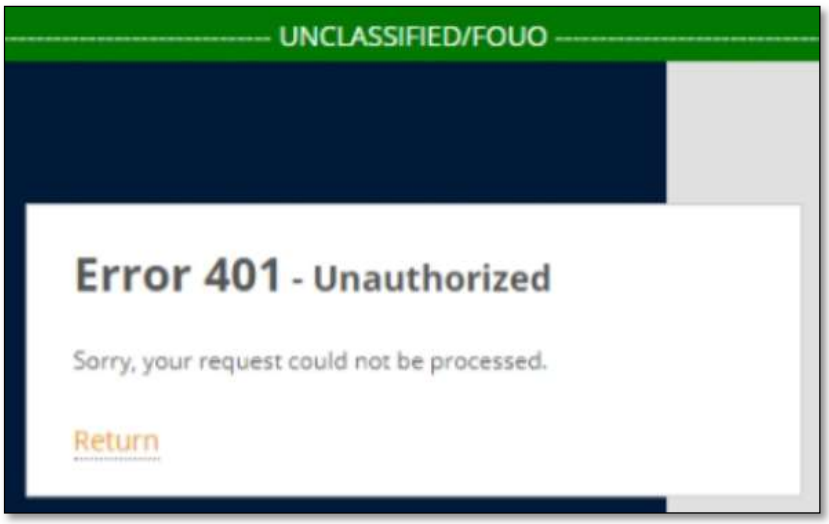
- Select New Access Request
- For Application Name, Select Check-In
- For Group Name, see Check-In Role Key at the end of this document for guidance
    - Note: CORs and PERSEC Approvers should first select NCI Approvers to select their group.
- Enter a justification statement and submit
- If more than one role should be requested, please submit a second request.
- You are all set! You will receive confirmation once your request is approved. Confirmation for contractors may take up to a week so that your documentation can be verified.

Note for Contractors: if you do not have a valid SAAR-N, please submit to your NAVWAR COR. Once signed, please send this and your IA Training Certificate to the IA office functional mailbox at: niwclant.issmops.fct@navy.mil. This will need to be sent through DoD SAFE.

Please know that SWAT Check-In Roles are separate from other applications, meaning if access to another application is needed, then you must submit a separate request for that application.

***

Result B: IF you receive the error below, please proceed to STEP B:



STEP B: Please email S2IPT Customer Support with the following:

Email: **s2iptcustsupport@spawar.navy.mil**
Subject: USER Add Request for SWAT
Body:

- EDIPI (please see the back of your CAC for the 10 digit number)
- First Name
- Last Name
- Email
- Phone
- Mobile

We will troubleshoot to let you know when you can verify login again. ***Once the issue is resolved, please return to this document and start at the beginning.***

Check-In Role Key

SWAT Check In app roles are split into two groups: "Customer Roles" and "Fulfillment Roles". Customer roles initiate and approve requests (Table 1). Fulfillment roles complete the associated tickets for each request (Table 2).

Table 1: Customer Roles

Customer Role Title	SWAT User Group	Responsibilities Within SWAT	Accessibility Within SWAT
Personnel Management Advisor (PMA)	NCI PMA	PMA user roles create all new government civilian personnel person records with Core and PII information. They have access to contribute profile information for new Person Record Profiles. PMAs have the ability to initiate and view requests.	The PMA can access all Person Records along with corresponding profiles and requests within the Check-In application for all personnel including government, military, and contractor personnel. PMAs may also initiate requests.
Supervisors	NCI Supervisors	Supervisor user roles initiate and approve requests for military and government personnel. When applicable, they will also be required to update newly created government civilian profiles once the PMA has initiated the creation of a Person Record Profile. If you are also a Hiring Manager, please also request the Hiring Manager role.	Supervisors may access profiles and requests for instances they support, present and historically, for government and military personnel. Supervisors may initiate and approve requests.
Hiring Manager	NCI Hiring Manager	In cases where a supervisor may not yet be assigned, the Hiring Manager may be required to take on the role of Supervisor for an employee (see Supervisor role description). If you are also a Supervisor, please also request the Supervisor role.	Hiring managers have access for instances they support, present and historically, for government and military personnel. Hiring Managers may also initiate requests.
Contractor Point of Contact (POC)	NCI Contractor POC	The Contractor POC is responsible for initiating requests for contractor personnel. At the time a Check-In Request is initiated, the user will be required to include information for a Person Record and Person Record Profile to be created. Users in this group should be Contractors only.	Contractor POCs can initiate requests and have access to profiles and requests they initiate and/or support, present and historical.
Contracting Officer (COR)	NCI COR	The COR is responsible for contractor personnel requests.	CORs may access profiles and requests for instances they support, present and historical. CORs may initiate and approve requests.
Personnel Security PERSEC (please see both	NCI PERSEC	PERSEC is responsible for approving contractor and military personnel Check-In	PERSEC will have access to view all Person Records, Person Record Profiles, and

PERSEC roles in Table 1 and Table 2)		requests, as related to security access information.	associated requests within the tool so that responsibilities can be carried out accordingly.
Civilian or Military Request Initiators	NCI Request Initiator	Access to submit a Check-In or Move Add Change (MAC) Request for Civilian and Military Personnel. When applicable, admins may also be required to update newly created government civilian profiles once the PMA has initiated the creation of a Person Record Profile.	Request Initiators have access to profiles and requests they support, present and historical.

Table 2: Fulfillment Roles

Fulfillment teams will have access to view all Person Records, Person Record Profiles, and associated requests within the tool so that responsibilities can be performed without hindrance.

Fulfillment Team Role Title	SWAT User Group	Responsibilities Associated with Check-In and MAC Requests
Trusted Agent (TA)	NCI Trusted Agent	Manage the DoD Common Access Card (CAC) for government and contractor personnel. The Common Access Card (CAC) is the principal card enabling access to buildings, facilities, installations, ships, and networks throughout DoD and DoN.
Access Control (AC)	NCI Access Control	Oversee NIWC Facility Access.
Command Information Systems Security Managers (ISSM)	NCI ISSM	Responsible for enforcing user compliance with IA Training certification, submission of user System Authorization Access Request Navy (SAAR-N), and other required documentation for NIWC IT Network access.
Personnel Security (PERSEC) (please see both PERSEC roles in Table 1 and Table 2)	NCI PERSEC Fulfillment	Validates employment eligibility to onboard and security access for NIWC IT Network on the SAAR-N.
Space Management	NCI Space Management	Locates and assigns physical space.
Telephony Operations	NCI Telephony	Assigns a desk phone number and voicemail.
Navy Marine Corps Intranet (NMCI) Accounts and Services	NCI NMCI Assets and Accounts	Assigns navy.mil email account and NMCI Assets depending on UIC.
Accounts Management	NCI Accounts Management	Issue NAVWAR LDAP account and facilitate changes associated with personal information and/or accounts.
ERP User Management	NCI ERP User Management	Facilitate provision of Navy ERP accounts and associated roles.
Research, Development, Test & Evaluation (RDT&E)	NCI RDT&E	Responsible for transfer and setup of RDT&E assets.
Task Administrator	Fulfillment Teams Only	Allows access to the tasks queue tab.