**OVERVIEW FOR USERS:**

CNIC FFR has implemented new CNIC FFR Systems Access Request Form that will replace individual application change forms & SAAR-N.

Beginning immediately, this form is to be used for N946 account requests and submitted via [support@aimshelp.com](mailto:support@aimshelp.com)

* The SAP Helpdesk email address - [mill\_mwr\_saphelpdesk@navy.mil](mailto:mill_mwr_saphelpdesk@navy.mil) – will no longer be monitored and user will be directed to [support@aimshelp.com](mailto:support@aimshelp.com)
* The CYMS Helpdesk email address - [Mill\_MWR\_CYMSHel.fct@navy.mil](mailto:Mill_MWR_CYMSHel.fct@navy.mil) – will no longer be monitored and users will be directed to [support@aimshelp.com](mailto:support@aimshelp.com)
* SAP HR Helpdesk - [mill\_mwr\_saphrhd.fct@navy.mil](mailto:mill_mwr_saphrhd.fct@navy.mil) – still active
* Kronos Helpdesk - [MILL\_MWR\_KronosH.fct@navy.mil](mailto:MILL_MWR_KronosH.fct@navy.mil) – still active

**NOTE – the SAP HR & Kronos Helpdesks listed above are NOT for application related issues.**

**NO HANDWRITTEN OR SCANNED COPIES WILL BE ACCEPTED**

---------------------------------------------------------------------------------------------------------------------

Section 1. User Information

Section 2. Request Type

Section 3. CYMS

Section 4. Kronos

Section 5. SAP

5.1 SAP ERP

5.2 FFR SAP PORTAL & BW

5.3 SAP HR

Section 6. Navy Single Sign On

Section 7. CNIC N9 GOVCLOUD

Section 8. Network Applications

Section 9. Completion of Background Investigation and Annual Training

Section 10. Special Instructions/Additional Details

Section 11. User Agreement & Approval Information

Section 12. Privileged Access Agreement & Approval Information

**Details for each Section**

Section 1. User Information

* Below information mandatory:
  + Given Name
  + Phone
  + Email
  + Job Role
  + Department
  + Program
  + Region

Section 2. Request Type

* **Initial Request** – (NEW ACCOUNT REQUEST)
  + **List the CITRIX ID if user has a CITRIX account. If not, this will initiate a request for a new CITRIX account.**
  + Select an application (Section 3, 4, 5, 6, 7 or 8)
  + Section 9 – Cyber Awareness & OPSEC and Date of Background Investigation & Security Manager Name must list completion dates for all NEW CITRIX ACCOUNT REQUESTS
    - Date of Background Investigation & Security Manager Name – use the same procedure as you did with a SAAR-N. More info below on Section 9
  + Section 11 is signed and dated by user and approving authority (Approver is the manager/supervisor approving you to get the account)
    - Must be digitally signed.
    - “Signature of IAM” is the CNIC IAM (Information Assurance Manager). DO NOT SIGN IN THIS FIELD
* **Modification** – (MODIFICATION OF ACTIVE ACCOUNT)
  + List current CITRIX user ID is (not required for SSO or JIRA)
  + Select the application that requires modification or list details in Section 10 (this area is for details/special instructions)
  + Section 9 – Cyber Awareness & OPSEC and Date of Background Investigation & Security Manager Name must list completion dates.
    - Date of Background Investigation & Security Manager Name – use the same procedure as you did with a SAAR-N. . More info below on Section 9
  + Section 11 is signed and dated by user and approving authority (Digitally)
    - Signature of IAM” -- CNIC IAM (Information Assurance Manager) will complete this portion - DO NOT SIGN IN THIS FIELD
* **Reactivate** – (IF ACCOUNT IS DISABLED)
  + List CITIRX user ID (even if it was disable – not required for SSO or JIRA)
  + Select the application that needs to be reactivated or details in Section 10 – If CITRIX was disabled – LIST IN SECTION 10
  + Section 9 – Cyber Awareness & OPSEC and Date of Background Investigation & Security Manager Name must list completion dates.
    - Date of Background Investigation & Security Manager Name – use the same procedure as you did with a SAAR-N. . More info below on Section 9
* Section 11 is signed and dated by user and approving authority (Digitally)
  + - “Signature of IAM” -- CNIC IAM (Information Assurance Manager) will complete this portion - DO NOT SIGN IN THIS FIELD
* **Deactivate** – (IF ACCOUNT REQUIRES DEACTIVATION)
  + List CITIRX user ID (not required for SSO or JIRA)
  + Select an application or details in Section 10 (this area is for details/special instructions)
  + Section 11 is signed by manager – no need for employee to sign
* **Privileged Access** – (THIS WILL ONLY APPLY TO IT SPECIALISTS FOR ADMIN ACCOUNTS)
  + Only applicable to application listed in Section 8 – Network Applications
    - Section 9 – Cyber Awareness & OPSEC and Date of Background Investigation & Security Manager Name must list completion dates.
    - Date of Background Investigation & Security Manager Name – use the same procedure as you did with a SAAR-N. . More info below on Section 9
  + Section 11 & 12 is signed and dated
    - Signature of IAM” -- CNIC IAM (Information Assurance Manager) will complete this portion - DO NOT SIGN IN THIS FIELD

Section 3 – CYMS

* Verify role is selected

Section 4 – Kronos

* Check mark if applicable. Kronos application access must be obtained through your local HR Department.

Section 5 – SAP

* Verify role is selected

Section 6 – Navy SSO

\*\*NOTE - This form is NOT required for password resets.

Selected – ADD or DELETE

* + CYP – Used by Marketing CYP Personnel ONLY
  + Marketing – for Marketing personnel ONLY
  + Movies – for Movie personnel for internal scheduling
  + Training – for HQ Training personnel ONLY
  + FITNESS (NFDMS- Navy Fitness Directors Management System)
    - New Accounts should be approved by Ira Seth ([navymwrfitness.fct@navy.mil](mailto:navymwrfitness.fct@navy.mil))
  + MTP – (Military Ticketing Program) for TMS MANAGER Access
    - ITT staff accounts must be created by their Manager.

\*\*\*NOTE - Multi-Roles can be requested in the “List Job Roles” field

Section 7 – CNIC N9 GOVCLOUD - used by HQ/Internally

* JIRA
* CONFLUENCE
* MEDIA MANAGER

Section 8 – Network Applications

* Will be selected in conjunction with Section 2 – Request Type

Section 9 – Completion of Background Investigation & Annual Training

* Cyber Awareness & OPSEC completion dates
* Date of Background Investigation & Security Manager Name – use the same procedure as you did with a SAAR-N. If it’s “in process” – list that in the date field.
  + CYP requestors who uses CSO to complete your background investigations – if you do not know who is/has conducted your investigation; you may list your local HR Rep in the “Security Manager Name” field. Contact them for date. Please note in Section 10 that CSO is the agency conducting background investigation and the HR Rep’s email and phone number.
  + Local Nationals – If a Local National does not have an official “Background Investigation” date, they may list the date that the local police department conducted a “police check” (background verification) prior to the local national being hired. Contact their local HR department if unsure of the date, as they have it on file, and list Police Cehck

Section 10 – Special Instructions/Additional Details

* Can be used in conjunction with any other field. May be used to note background investigating “in process”, etc. or for other application requests NOT listed in other sections.

Section 11 – User Agreement & Approval Information

* Both requestor and Approver information is required (whoever is approving new requests or make changes to the user account)
* Signature of IAM or Appointee – CNIC IAM (Information Assurance Manager) will complete. DO NOT SIGN IN THIS FIELD
* Will only accept digital signatures.
  + If requester does NOT have a CAC ID – send a ticket into AIMS support and ask them to send the instructions on “How to create a Digital Signature without a CAC”

Section 12 - Privileged Access Agreement & Approval Information

* ONLY Required if Section 2 – Privileged Access is checked
* THIS WILL ONLY APPLY TO IT SPECIALISTS FOR ADMIN ACCOUNTS