|  |  |  |
| --- | --- | --- |
| **Name:** | **Date of Departure:** | |
| **Rank/Grade** | **Office Symbol:** | |
| **Supervisor:** | **Reason Out-Processing:** | |
| **\*\*Not to be accomplished by EPASS (A&AS) Contractors** | | |
| **ALL P1 Personnel** | | |
| **Action** | | **Date/Int’l** |
| **MM & Confluence Access:**  **Basic IL2 Access Request**   * Complete the Cyber awareness Training (<https://lms-jets.cce.af.mil/moodle/course/view.php?id=12980>) * Visit https://login.dso.mil * There's a spot that says "No account? Click here to register now.", that will allow you to create an account in a self service manner. * Use your work or .mil email to sign up. Signing up with a .mil email is preferred as doing so will automatically associate your account with a group authorized to access IL2 and IL4 resources.   **Team Lead IL2 Access:** *(For personnel requesting access for members they manage)*   * Complete Basic Access request steps and provide a 2875 signed by your Value Stream Team lead or appointed rep.   **IL2/IL4 Access Request**   * Contract Personnel: Complete Basic Access request and team lead steps. * [Complete Controlled Unclassified Training](https://lms-jets.cce.af.mil/moodle/course/view.php?id=11998) (CUI) * Visit <https://chat.il4.dso.mil> to create your IL4 account.   **Note**: Utilize the MM Walk-through for account creation assistance: [Platform One SSO (dso.mil)](https://sso-info.il2.dso.mil/new_account.html)   * Once Complete, notify your contract Contract Lead so they can s[ubmit Internal Onboarding ticket to gain](https://jira.il2.dso.mil/servicedesk/customer/portal/1/create/497) [access to Confluence](https://jira.il2.dso.mil/servicedesk/customer/portal/1/create/497)/Jira | |  |
| **Contract Personnel CAC Card Issuance**  **(***N/A to EPASS Contractors)*  CAC's WILL NOT be processed for any employee on contract that doesn't have at a minimum a Federal Bureau of Investigations (FBI) Fingerprint Check and a National Agency Check with Written Inquiries (NACI) check.   * Please find full details, CAC requirements, and POCs here. | |  |
| **COMM Equipment Issuance: Will be issued by Servicing Company** | |  |
| **ZOOM Accounts Creation:** Zoom account creation requests must be approved and submitted by your Value Stream Lead to P1 Ops Team  \*\*Specify whether member needs a zoom basic or zoom pro\*\* | |  |
| **NIPR Acct Provision (If Applicable)**: Accomplish the forms identified below for account provision. Provide them to your VS lead for processing.   * 2875 * **Section 13 MUST Include:** Request NIPR account. Individual is a non-A&AS, non-FFRDC contractor and as such should not be given shared drive accesses. Basic email and personal drive (Z:) will be sufficient * AF User Agreement * Rules and Behavior   AFLCMC NIPR Docking Agreement | |  |

**CAC Card Issuance**

**Prerequisites/Process - Background Investigation**

**CAC's WILL NOT be processed for any employee on contract that doesn't have at a minimum a Federal Bureau of Investigations (FBI) Fingerprint Check and a National Agency Check with Written Inquiries (NACI) check**

**Employee currently doesn’t possess any of the checks listed above then either a T1(Unclassified), T3 (Secret), or T5 (Top Secret) background investigation will need to be initiated**

T1's are only initiated for personnel from your company IAW the contract requirements as not needing classified access throughout the duration of the contract to Secret and Top-Secret information

* T1's are only needed for employees that don't have a NACI & FBI Fingerprint check already in place
* Background Check determination – T1 (Unclassified) - (CUI) T1 Submission Request Form.docx
* If your contract has no classified requirements, then it will be Platform One's responsibility to initiate a T1 Background on behalf of your employee if needed

Background Check determination – T3 (Secret), T5 (Top Secret)

* Contract identifies classified requirements: Employees company **must** initiate either a T3 or T5 investigation on behalf employee
* **Note**: Please do not submit or inform your employee to submit an CAC application until their investigation is open, and they’ve submitted their fingerprints
* Failure to accomplish previous step will result in the application being put on hold by the Platform One Security Manager until complete.

**CAC Applications for Employees with Background Check in DISS**

1. Complete Section One of TASS Application
   1. **NOTE**: Ensure you use Acrobat Standard or Pro, or Foxit to save information into the form..
2. Identify appropriate Contract COR in block 16,
   1. Contract COR can be found here:
3. Contract lead verifies data send completed forms via .mil email to Platform One TA’s to ensure for processing.
4. **DO NOT** send forms via personal email as it contains PII. Please send passphrase to TA via direct message on MM on IL-4 or .mil email.
5. TA will endorse (Section Two) **only** if employee has been verified via the company’s roster found on the contract rosters
6. TA will place form in the Platform One Security Manager folder for security verification.
7. Platform One Security Manager will verify clearances and if member is authorized CAC. Once confirmed, endorse (Section Three) and place application in to the TA's folders for action
8. TA’s will process CAC for employee and communicate credentials via email to employee
9. Employee needs to submit application within 7 days or it will expire, when submitted TA will approve
10. Employee may now proceed to a RAPIDS location and go pick up CAC card

**CAC Applications for Employees with no Background Check in DISS**

If employee is identified to be on a contract with no classified requirements, and currently has no background check information found in DISS, then:

1. Contract COR must agree to sponsor a background check on behalf of the new employee. Platform One security manager will add employee to the ~~Platform One~~ T1 list after receiving once they’ve received said concurrence.
2. Contract Lead will send the attached form via .mil to all three TA’s & Platform One Security Manager
3. Once concurrence is received by COR, HNCX Security Manager will submit a T1 request for employee up to the AFLCMC/HNC-SO
4. Employee will not be issued a CAC until background check is completed. Once complete, COR/TA will submit the employee for a CAC.

If employee is identified to be on a contract with classified requirements, and currently has no background check information found in DISS, then:

1. Platform One security manager will place their CAC application in a hold status until T3 or T5 investigation can be completed by their company.
2. It is the company’s responsibility to expediate submission of their employee through the T3 or T5 investigation process
3. CAC applications will be in this “hold” state and checked bi-weekly on Friday’s by the Security Manager to determine if “background investigation show’s open”
4. Once investigation “shows open” CAC application will be moved to TA’s folder for processing