

Vantage Account Request Instructions for Command Teams and Staff w/ Risk Reduction

The Commander's Risk Reduction Toolkit (CRRT) is currently only available to Command Teams and Staff who are CRRD Inc II Users and pre-approved users.

These are general instructions for how to request an account to Army Vantage. If you have any questions, please contact usarmy.vantage.support@mail.mil

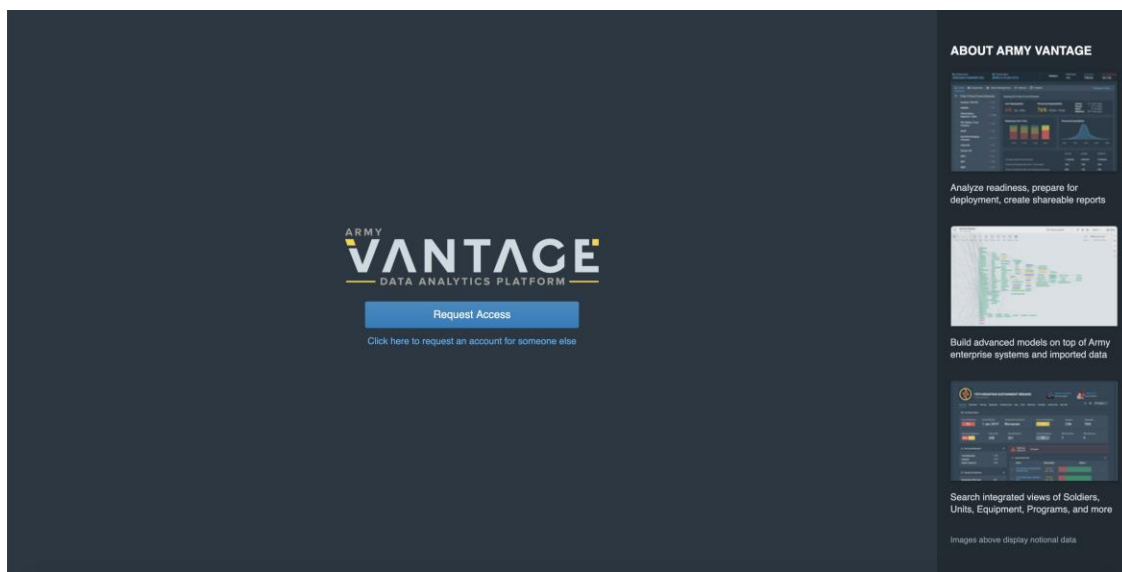
Vantage Account Request Instructions

1. With your CAC inserted, navigate to the Army Vantage site on NIPR:

<https://vantage.army.mil/>

*Note that Army Vantage is optimized for Chrome and Firefox browsers. **You will not be able to complete the registration process if you use Internet Explorer.** If the page does not load, please check to see that you are VPN'd into the government network. If you are using Firefox, please also ensure that your Firefox browser is CAC-enabled.*

You will see a screen like the one below when you visit the Vantage home page:



2. On the splash page, click on the button to “Request Access”

This will bring you to the registration page. Registration includes a series of steps to ensure your account has the correct information.

Please note that you will need to complete the **Cyber Awareness training and upload a PDF of your certificate of completion** as part of the account request process. You will receive an error message if you have not uploaded your Cyber Awareness certificate.

To complete your Cyber Awareness Training please follow the steps below:

1. You can access the training module at the following link:
<https://cs.signal.army.mil/>
2. Follow the instructions to log in and click "Cyber Awareness" at the top to begin the training
3. Save a PDF of your certificate on your desktop so you can upload this document as part of your account request

For access to PII (e.g., Command teams users that will need regular access to Soldier-level data), you will also need to complete the **Safeguarding PII training and upload a PDF of the certificate of completion** for this training as well.

Please note:

- If you have previously taken HIPPA training that covers PII, you can substitute the HIPPA certificate for the Safeguarding PII certificate.
- If you have taken the Privacy Overview Act training from the Army's Learning Management System (ALMS at <https://www.lms.army.mil>), you can substitute it for the Safeguarding PII certificate.
- If either of your HIPPA or Privacy Overview Act training certificate is within 30 days of expiration, Safeguarding PII training certificate is required.

To complete your PII training please follow the steps below:

1. You can access the training module at the following link:
<https://cyber.mil/training/identifying-and-safeguarding-personally-identifiable-information-pii/>
2. Log in to the DOD Cyber Exchange using your CAC when prompted with the USG Warning and Consent Banner (note: it may prompt you to authenticate with your PIN more than once)
3. On the DOD Cyber Exchange page, click "Launch Training"
4. Select "Start/Continue Identifying and Safeguarding Personally Identifiable Information (PII)"
5. Complete the video training

6. Save a PDF of your certificate on your desktop so you can upload this document as part of your account request

Request Access to Army Vantage [Need Help?](#)

Progress

- [Overview](#)
- [Personal Information](#)
- [Access Information](#)
- [Training Certificates](#)
- [Acceptable Use Policy](#)
- [Review and Submit](#)

Overview

Completing this form will submit a request for access to Army Vantage, the Army's Data Analytics Platform.

Please read through the following section to determine the materials you will need to have available on your computer before you begin

What you will need:

- 1. Cyber Awareness training certificate in PDF format** dated within the last year.
You will need to be able to upload this document as part of your account request.
[If you need to complete this training, click here.](#) [Estimated 1 hour]
- 2. Name, email, and phone number for your Commander, Supervisor, or Sponsor**
- 3. The Unit Identification Code (UIC)** for the Unit for which you are requesting access
- 4. If you require access to Personally Identifiable Information (PII) for Soldiers, you will need the Safeguarding Personally Identifiable Information (PII) training certificate in PDF format** dated within the last year.
You will need to be able to upload this document as part of your account request.
[If you need to complete this training, click here.](#) [Estimated 1 hour]

[Continue](#)

3. Fill out the personal information section.

You will notice that some information will have been pre-populated in the form. This information is being pulled from your CAC. Please ensure this information is correct before clicking “continue”. You will need to complete all fields.

In the Unit Identification Code (UIC) field, **please input the UIC of the Unit you**

command (if you are a member of a Command Team) or of the Unit you support (if you are a Staff member). For example, Battalion Commanders should specify their Battalion UIC (i.e., WXXXAA), not their assigned Company UIC (i.e., WXXXT0).

Request Access to Army Vantage

Need Help?

Progress

Overview

Personal Information

Access Information

Training Certificates

Acceptable Use Policy

Review and Submit

Enter Personal Information

All fields must be complete in order to move on to the next page.

Full Name

e.g. John Doe

Title / Billet

e.g. XO to G-2

Email Address

Select A Designation:

☐ Military ☐ Civilian ☐ Contractor

Country of Citizenship

DoD ID Number

Unit Identification Code (UIC) / Organization

Provide the UIC at the level of access (Company, Battalion, etc.) required.
e.g. Battalion Commanders should specify their Battalion UIC (i.e. WXXXAA), not
their assigned Company UIC (i.e. WXXXT0)

Enter Commander Information

The listed individual may be contacted for verification of any of the
information provided during registration.

Commander Name

Commander Email

Commander Phone

Back

Continue

4

4. Fill out the Access Information section.

For **Assignment**, select the DOD organization to which you are currently assigned.

For **Program Affiliations**, please select "**Command Teams and Staff with Risk Reduction.**"

For **Installation**, please select the installation where you are located or the installation that provides Risk Reduction support to your unit if located off an Army/Joint base.

For **Level of Access**, please select "**Sensitive Data**" if you require elevated access (intended for unit commanders and supporting staff). In the next dropdown, select "**Sensitive Soldier Data for my Unit**" which will provide access to sensitive soldier and unit data for your UIC and all subordinate units (as determined by the UIC provided in the previous Personal Information section). You must maintain updated Safeguarding PII certification to remain active. If you do not require access to PII (example: Supply Sergeants, Maintenance Officers), please select "**Basic Soldier Data**" for the standard access level to Vantage.

For **Role Description**, please input a description of your current role and **specify whether you are either an existing CRRD Inc II user or are one of the pre-approved users.** (e.g., "I am a Battalion Commander and CRRD Inc II user." or "I am a Company Commander at the 82nd Airborne Division").

Request Access to Army Vantage

[Need Help?](#)

PROGRESS

Overview ✓

Personal Information ✓

Access Information ✓

Training Certificates

Acceptable Use Policy

Review and Submit

Assignment

Select the DOD organization to which you are currently assigned.

Department of the Army

Program Affiliations

Select the current Vantage program you are using in your role. Please note that Vantage access is currently limited to several programs. If you do not see your program on this list or are unsure which program affiliation to select, please check with your commander or team lead.

Command Teams and Staff with Risk Reduction

Installation

Select the installation to which you are assigned.

Your designation is Military

What level of access to Soldier data do you require?

Please note: requesting access more sensitive than necessary will result in a rejected access request.

Basic Soldier Data

Name, rank, MOS/AOC, and assigned unit.

Sensitive Data

(Recommended for Command Teams, Staff, Unit Leaders, etc. If you request sensitive data access, you must provide your reason for need to know at the level requested in the role description below.)

Basic Soldier data along with health, training, and personal data.

What level of Sensitive data do you require?

Sensitive Soldier Data for my Unit

UIC: WXXXT0

Sensitive Soldier Data for the Army

⚠ Restricted Access

Role Description (Required: explain need to know for sensitive access)

I am a Battalion Commander.

[Help?](#)

Back

Continue

5. Upload your Cyber Awareness certificate.

Submit a PDF of the certificate you received upon completion of your Cyber Awareness Training. Cyber Awareness Training is available

at <https://public.cyber.mil/training/cyber-awareness-challenge/>. The link is also available directly in the platform.

Cyber Awareness Training [Estimate 1 hour]

All new accounts are required to upload a certificate of completion from the **DoD Cyber Awareness Challenge**, dated within the last year.

If you need to complete this training, [click here](#)



Drag-and-drop file here
or [choose from your computer](#)

Please manually verify the date of completion below


6. If you have requested access to Sensitive Data, upload your Safeguarding PII certificate.

Safeguarding PII training is available at <https://cyber.mil/training/identifying-and-safeguarding-personally-identifiable-information-pii/>. The link is also available directly in the platform.

PII Training [Estimate 1 hour]

All new accounts are required to upload a certificate of completion from the **Safeguarding Personally Identifiable Information (PII) training**, dated within the last year.

[If you need to complete this training, click here](#)



Drag-and-drop file here
or [choose from your computer](#)

Please manually verify the date of completion below

MM/DD/YYYY

7. Read and acknowledge the Army Vantage Acceptable User Policy

8. Review your information

Please review the information in your request carefully before submitting. In particular, please confirm that the UIC you provided is for the echelon that includes all of the data that you require access to. For example, Battalion Commanders should specify their Battalion UIC (i.e., WXXXAA), not their assigned Company UIC (i.e., WXXXT0).

Incorrect information may result in your request being denied. Once you submit your request, you will NOT be able to modify your information until your account is approved or rejected.

9. Submit your request

Your request will be reviewed by the Vantage Program Team. Request processing can take several days to complete. If there are any mistakes in or questions about your request form, a member of the Vantage team may reach out to you for corrections. If your request is denied due to incorrect information, you can resubmit a new request with the correct information.

10. After completing this process for NIPR, if you would also like to request a SIPR account please complete the same process on SIPRnet by navigating to <https://vantage.army.smil.mil/>

You will not be requested to upload any certificates as part of the SIPR process since your certificates will already be on file via the NIPR account provisioning process.

Please note: Accounts will auto-disable after 30 days of inactivity. On the Vantage home page, you will be able to click on “Request Reactivation” and follow the steps to get your account reactivated!