



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

NBIS INDUSTRY ONBOARDING READINESS CHECKLIST

A minimum of two (2) cleared Industry Onboarding Managers are required from each company holding a Facility Clearance to complete the NBIS Industry Onboarding process in order to be provisioned access to the NBIS system. The Industry Onboarding Readiness Checklist, as detailed below, provides a checklist of items required to be completed as part of the Industry Onboarding process.

Industry Partners can review and complete this checklist now. Once the Industry Onboarding begins, Industry will be able to submit the checklist requirements in the future NBIS Industry Onboarding Portal.

✓	NBIS REQUIREMENT	DESCRIPTION	ATTACHMENT
☐	Identify 2 representatives from your company	Identify 2 representatives who will complete the designated tasks; check box once completed	N/A
☐	Compatibility of Internet Browser(s)	Confirm use of the most recent versions of at least one of the following: Mozilla Firefox (Recommended); Google Chrome (Recommended); or Microsoft Edge; check box once completed <i>Note - Google Chrome and Mozilla Firefox should be utilized to access the NBIS System whenever possible.</i>	N/A
☐	Minimum Investigation Requirement	Confirm National Industrial Security Program (NISP) Industry Contractor users have a minimum of an adjudicated T3 investigation; check box once completed	N/A
☐	Common Access Card (CAC), Personal Identity Verification (PIV), or External Certification Authority (ECA)	Confirm NBIS users have the necessary smartcard for identity authentication; check box once completed	N/A
☐	Cybersecurity Training	Review guidance and complete the Cybersecurity training (within the past 12 months); save certificate and check box once completed	
☐	Personally Identifiable Information (PII) Training	Review guidance and complete PII training (within the past 12 months); save certificate and check box once completed	





DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

NBIS INDUSTRY ONBOARDING READINESS CHECKLIST

BROWSER REQUIREMENT

The NBIS System is accessed through a web-based application that requires a supported Internet browser. The NBIS System must be accessed using the latest versions of the following browsers:

- **Mozilla Firefox (Recommended);**
- **Google Chrome (Recommended);** or
- Microsoft Edge

Note - Google Chrome and Mozilla Firefox are the recommended browsers and should be utilized for NBIS whenever possible.

STEPS FOR COMPLETION:

- **Step 1:** Verify with your IT Department, or appropriate designee, that your information system has at least one of the above listed compatible browsers and that it is updated to consistently run the latest version.
- **Step 2:** If not, obtain access to one of the above listed compatible browsers.
- **Step 3:** Check the box for 'Compatibility of Internet Browser(s)' in the Industry Onboarding Readiness Checklist to confirm completion of requirement.

NBIS SYSTEM MINIMUM INVESTIGATION REQUIREMENT

A minimum of a 'favorably' adjudicated Tier 3 (T3) background investigation is required for access to the NBIS System. Additionally, any user with the permission of Initiate and/or Review within the NBIS System will also require a favorably adjudicated T3 background investigation. Please note that while future NBIS System capabilities may require a higher Tier background investigation, a higher tier is not needed at this time.

STEPS FOR COMPLETION:

- **Step 1:** Validate that you have a favorably adjudicated T3 background investigation clearance by confirming with your company's security office or project point of contact. Ensure that this verification can be tracked in writing, as needed.
- **Step 2:** Check the box for 'Minimum Investigation Requirement' in the Industry Onboarding Readiness Checklist to confirm completion of requirement.





DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

NBIS INDUSTRY ONBOARDING READINESS CHECKLIST

CAC / PIV / ECA REQUIREMENT

NBIS System users must have one of the following secure authentication methods to verify identification when accessing the system:

- **Common Access Card (CAC):** This standard 'smart' card is used to enable physical access to buildings and controlled spaces and grants access to DoD-secured networks and systems. Note that some desktops/laptops do not have an Integrated CAC Reader, in which case, an external CAC Reader is necessary.
- **Personal Identification Verification (PIV):** This 'smart' card must be Public Key Infrastructure (PKI)-enabled and federally compliant. More information on Public Key Infrastructure/Enabling (PKI/PKE) located here: <https://public.cyber.mil/pki-pke/>
- **External Certification Authority (ECA):** These 'smart' cards are managed by The DoD ECA program and ECAs are DoD-approved certificates that are issued to industry partners and other external entities and organization. The program is designed to provide the mechanism to securely communicate with DoD and authenticate to DoD Information Systems. More information and approved ECA Vendors located here: <https://public.cyber.mil/eca/>

STEPS FOR COMPLETION:

- **Step 1:** Understand which authentication method is used by your facility.
- **Step 2:** Obtain the identified authentication method, if not already obtained.
- **Step 3:** Confirm validity of current authentication card by ensuring the smart card is not expired and has necessary certifications. If expired or missing certifications, address with your company's Facility Security Officer.
- **Step 4:** Check the box for 'CAC/PIV/ECA' in the Industry Onboarding Readiness Checklist to confirm completion of requirement.

CYBERSECURITY TRAINING

For provisioning to the NBIS System, all users must complete the Cybersecurity training within the last 12 months. To provide proof of completion, the DoD Cyber Awareness Challenge Training Certificate will be uploaded as a PDF attachment to the Industry Onboarding Readiness Checklist.

Note: While the initial users of a given company must complete this training, all users seeking provisioning to the System must also submit a completed certificate with the PSSAR form prior to access being granted to the NBIS System.

STEPS FOR COMPLETION:

- **Step 1:** Complete the 1-hour DoD Cyber Awareness Challenge Training, which can be accessed through one of the below course catalogs:
 - CAC users: <https://cyber.mil> (From the homepage, click the 'Training' dropdown, and select 'Cyber Awareness Challenge')
 - All other users: <https://public.cyber.mil/training/cyber-awareness-challenge/>
- **Step 2:** Once completed, you will receive a certification message within the browser screen itself. This information will include your name and the date of completion. Download this certificate as a PDF file.
- **Step 3:** Save the certificate and prepare for uploading into the NBIS Industry Onboarding Portal, when available.





DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

NBIS INDUSTRY ONBOARDING READINESS CHECKLIST

PERSONALLY IDENTIFIABLE INFORMATION (PII TRAINING)

For provisioning to the NBIS System, any user must complete a Personally Identifiable Information (PII) training within the last 12 months. To provide proof of completion, the DoD PII Training Certificate must be uploaded as a PDF attachment into NBIS Industry Onboarding Portal, when available.

Note: While the initial users of a given company must complete this training, all users seeking provisioning to the System must also submit a completed certificate with the PSSAR form prior to access being granted to the NBIS System.

STEPS FOR COMPLETION:

- **Step 1:** Complete the DoD PII Training (est. time of 1-hour to complete), which can be accessed via the following site: <https://securityawareness.usalearning.gov/piiv2/index.htm>
- **Step 2:** Once completed, you will receive a certification message within the browser screen itself. This information will include your name and the date of completion. Download this certificate as a PDF file.
- **Step 3:** Save the certificate and prepare for uploading into the NBIS Industry Onboarding Portal, when available.

