Office of the Assistant Secretary – Indian Affairs
Bureau of Indian Affairs
Bureau of Indian Education

NEW CONTRACTOR/VOLUNTEER	
Office:	
Name:	
Address:	
Telephone number:	
Email:	
Entry on Duty:	
Contractor PM:	
COR Representative:	

Note: Follow the **“Indian Affairs Identity Credential and System Access Checklist” attached**. This includes DOI Access, acquiring a computer, etc.

CHECKLIST			
COR	☐	Notification date	Email notifying new employee.
	☐	Employee Badge	The badging process may take several weeks to complete. The new employee may need to obtain a temporary badge on the first day. In order to access your laptop, you will need your employee badge.
	☐	Enter employee in IIS	DOI Access will populate the user's profile into IIS once the Adjudication Status date is completed.
SET-UP RESOURCES			
COR/Contractor PM	☐	Federal Information Systems & Security Awareness + Rules of Behavior	This process begins before employee’s first day. Email information on how to access training and complete it prior to first day.
	☐	Submit Non-disclosure agreement	
	☐	Identify and prepare employee’s work area	Room and phone number: _______________________________ ☐Office keys. ☐Prepare office space.
	☐	Request computer workstation	Acquire computer with property tag two weeks prior to start date. See table below for more information.
	☐	Telework ☐ YES ☐ NO	YES – Request VPN Remote Access in Identity Information System (IIS). Bring the computer to an Indian Affairs (IA) site for configuration before initiating telework. Then the user must log on to a DOI network initially.

Indian Affairs Identity Credential and System Access Checklist

	ACTION	HR	Individual	Supervisor / COR	Personnel Security	System Business Owner/ System Administrator	Office of Information Technology Management
1	The Contracting Officer Representative (COR) completes AS-IA/BIE/BIA Background Investigation Process request form and emails the form to the Personnel Security Office. AS-IA: lynn.mccullough@bia.gov BIA: IA_Personnel_Security_BIA_eQIP@bia.gov BIE: biepersec@bia.gov OJS: IA_Personnel_Security_OJS_eQIP@bia.gov	**X**	**X**				
2	**AS-IA/BIA:** The COR goes to the DOI Access site at https://eprofile.ia.doi.net/, sponsors the individual, and directs the individual to the General Services Administration (GSA) Online Scheduling System, USAccess site at https://portal.usaccess.gsa.gov/scheduler/ to schedule an appointment at the USAccess facility for fingerprinting to meet the HSPD-12 card issuance requirements. **BIE:** The Personnel Security Office sponsors the individual and directs the individual to the GSA Online Scheduling System at https://portal.usaccess.gsa.gov/scheduler/ to schedule an appointment at the USAccess credentialing facility for fingerprinting to meet HSPD-12 card issuance requirements.	**X**		**X**	**X**		
3	**AS-IA/BIA:** The user coordinates with COR to go to FED ID Site for fingerprinting appointment. https://www.fedidcard.gov/home **BIE:** The user coordinates with the Personnel Security Office to schedule the fingerprinting appointment using the GSA Online Scheduling System https://portal.usaccess.gsa.gov/scheduler/ located on the Fed ID Card website https://www.fedidcard.gov/.	**X**	**X**		**X**		
4	Personnel Security Office receives background investigation request and then sends email to the individual to initiate the background investigation. Forms should be completed through the Office				**X**		

	ACTION	HR	Individual	Supervisor / COR	Personnel Security	System Business Owner/ System Administrator	Office of Information Technology Management
	Personnel Management (OPM) portal e-QIP site at https://nbib.opm.gov/e-qip-background-investigations/.						
5	Individual completes the investigative forms in the e-QIP system. If there are any additional forms required, then the individual will be contacted by email.		**X**				
6	Personnel Security Office releases the electronic fingerprints on file with DOI Access.				**X**		
7	If the pre-employment screening checks are favorable, Personnel Security Office updates the personnel security database and DOI Access with the favorable fingerprint review information so the individual can be allowed access to IA systems/facilities by their program sponsor/COR while the investigation is ongoing. The program sponsor/COR checks the DOI Access system for the status of an individual's fingerprint results.				**X**		
8	Personnel Security Office releases the forms electronically to the Defense Counterintelligence Security Agency				**X**		
9	COR must acquire the computer and ensure it has a property tag.			**X**			
10	Individual completes Federal Information Systems Security Awareness + Privacy and Records Management Training (FISSA+) at DOI Talent, https://doi.gov/doitalent/training-download. Certificate must be emailed to IIS government approver and HR staffing specialist. Contractor submits non-disclosure agreement.		**X**	**X**			
11	COR must request the system access for Active Directory and email in IIS two weeks before the individual's start date. If the system requires the client software, the program sponsor must open the Service Center ticket at servicecenter@bia.gov. **BIE Users:** Submit a BIE systems request form to BIE IIS designated approver. **Note:** IIS must be used to request IA systems access.			**X**			

	ACTION	HR	Individual	Supervisor / COR	Personnel Security	System Business Owner/ System Administrator	Office of Information Technology Management
12	Prepare and configure equipment (pre-staging).						X
13	Email notification from DOI Access to a supervisor/COR and OIMT system administrators when ready for the activation and provisioning of their Active Directory account.			X			X
14	System Business Owner must approve system access in IIS. **NOTE:** OIMT is not the System Business Owner for all Indian Affairs Systems. Other Program Managers are responsible for their respective system applications.					X	
15	System Administrator for the respective system must approve in IIS. **NOTE:** OIMT is not the System Administrator for all Indian Affairs Systems. Other Program Managers are responsible for their respective system applications.					X	
16	OIMT activates Active Directory and email account, approves IIS request, and notifies user.						X
17	Provide instructions/Training to user to the systems requested.					X	

NOTE:

- **Only Government Furnished Equipment** may be used to access Indian Affairs systems.
- COR must request the system access and Active Directory in IIS two weeks before the individual's start date. If the system requires the client software, the COR must open a Service Center ticket at sc.indianaffairs.gov or servicecenter@bia.gov.
- **DOI OCIO Directive 2012-007**: Personal Identification Verification Two-Factor Authentication for VPN Remote Access.
- **DOI** Rules of Behavior Bullet #10 (sign/certify annually).
- If you have any questions regarding this checklist, please contact the Service Center at sc.indianaffairs.gov or servicecenter@bia.gov.