#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.5	**Access Control**					
1.	Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information. Refer to CSP 5.13.6 for additional access control requirements related to mobile devices used to access CJI. Based on inquiry and record examination, does the Tribe or TGRA manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts?	____	____	____	CSP 5.5.1	
	Does the Tribe or TGRA validate information system accounts at least annually and document the validation process?	____	____	____	CSP 5.5.1	
2.	Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. Based on inquiry and record examination, does the Tribe or TGRA identify authorized users of the information system, and specify access rights/privileges?	____	____	____	CSP 5.5.1	
	Does the Tribe or TGRA grant access to the information system based on: 1. Valid need-to-know/need-to-share that is determined by assigned official duties?	____	____	____	CSP 5.5.1(1)	
	2. Satisfaction of all personnel security criteria?	____	____	____	CSP 5.5.1(2)	
	Are the person(s) responsible for account creation notified when: 1. A user's information system usage or need-to-know or need-to-share changes?	____	____	____	CSP 5.5.1(1)(1)	
	2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured?	____	____	____	CSP 5.5.1(2)(2)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
3.	Based on inquiry and record examination, does Tribe or TGRA's information system enforce assigned authorizations for controlling access to the system and contained information?	____	____	____	CSP 5.5.2	
	Do the information system controls restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel?[1]	____	____	____	CSP 5.5.2	
	Does the Tribe or TGRA employ access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system?	____	____	____	CSP 5.5.2	
4.	Based on inquiry and record examination, does the Tribe or TGRA approve individual access privileges and enforce physical and logical access restrictions associated with changes to the information system and generate, retain, and review records reflecting all such changes?	____	____	____	CSP 5.5.2.1	
	Does the Tribe or TGRA enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks?	____	____	____	CSP 5.5.2.1	
	Does the Tribe or TGRA implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI?[2]	____	____	____	CSP 5.5.2.1	
	Does the Tribe or TGRA maintain the logs of access privilege changes for a minimum of one year or at least equal to the agency's record retention policy- whichever is greater?	____	____	____	CSP 5.5.2.1	

[1] Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).
[2] This limits access to CJI to only authorized personnel with the need and the right to know.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.	Based on inquiry and record examination, does the Tribe or TGRA restrict by object (e.g., data set, volumes, files, records), including the ability to read, write, or delete the objects, the access control mechanisms to enable access to CJI?	____	____	____	CSP 5.5.2.2	
	Are access controls in place and operational for all IT systems to:					
	1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs?	____	____	____	CSP 5.5.2.2(1)	
	2. Document the parameters of the operational business needs for multiple concurrent active sessions?	____	____	____	CSP 5.5.2.2(1)	
	3. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs?	____	____	____	CSP 5.5.2.2(2)	
6.	Based in inquiry and record examination, does the Tribe or TGRA control access to CJI based on one or more of the following:					
	1. Job assignment or function (i.e., the role) of the user seeking access?	____	____	____	CSP 5.5.2.3(1)	
	2. Physical location?	____	____	____	CSP 5.5.2.3(2)	
	3. Logical location?	____	____	____	CSP 5.5.2.3(3)	
	4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside)?	____	____	____	CSP 5.5.2.3(4)	
	5. Time-of-day and day-of-week/month restrictions?	____	____	____	CSP 5.5.2.3(5)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
7.	Based on inquiry and record examination, does the Tribe or TGRA use one or more of the following mechanisms when setting up access controls:					
	1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted?	____	____	____	CSP 5.5.2.4(1)	
	2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices?	____	____	____	CSP 5.5.2.4(2)	
	3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management[3]?	____	____	____	CSP 5.5.2.4(3)	
	4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency?	____	____	____	CSP 5.5.2.4(4)	
8.	Based on record examination, where technically feasible, does the Tribe or TGRA require the system enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI)?	____	____	____	CSP 5.5.3	
	Does the system automatically lock the account/node for a 10 minute time period unless released by an administrator?	____	____	____	CSP 5.5.3	

[3] Follow the guidance in CSP 5.10.1.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
9.	Based on record examination, does the Tribe or TGRA's information system display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules?	____	____	____	CSP 5.5.4	
	Does the system use notification message, at a minimum, provide the following information:					
	1. The user is accessing a restricted information system.	____	____	____	CSP 5.5.4(1)	
	2. System usage may be monitored, recorded, and subject to audit.	____	____	____	CSP 5.5.4(2)	
	3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.	____	____	____	CSP 5.5.4(3)	
	4. Use of the system indicates consent to monitoring and recording.	____	____	____	CSP 5.5.4(4)	
	Based on inquiry and examination, does the Tribe or TGRA's system use notification message provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system?	____	____	____	CSP 5.5.4	
	Are privacy and security policies consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance?	____	____	____	CSP 5.5.4	
	Are system use notification messages implemented in the form of warning banners displayed when individuals log in to the information system?	____	____	____	CSP 5.5.4	
	For publicly accessible systems:					
	1. The system use information is available and when appropriate, is displayed before granting access?	____	____	____	CSP 5.5.4(1)(1)	
	2. Any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities?	____	____	____	CSP 5.5.4(2)(2)	
	3. The notice given to public users of the information system includes a description of the authorized uses of the system?	____	____	____	CSP 5.5.4(3)(3)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
10.	Based on record examination, does the Tribe or TGRA's information system prevent further access to the system by initiating a session lock[4] after a maximum of 30 minutes of inactivity?	____	____	____	CSP 5.5.5	
	Does the session lock remain in effect until the user reestablishes access using appropriate identification and authentication procedures?	____	____	____	CSP 5.5.5	
	Do users directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended?	____	____	____	CSP 5.5.5	
	Note: an example of a session lock is a screen saver with password.					
11.	Based on inquiry and record examination, does the Tribe or TGRA authorize, monitor, and control all methods of remote access[5] to the information system?	____	____	____	CSP 5.5.6	
	Based on inquiry and record examination, does the Tribe or TGRA employ automated mechanisms to facilitate the monitoring and control of remote access methods?	____	____	____	CSP 5.5.6	
	Does the Tribe or TGRA control all remote accesses through managed access control points?	____	____	____	CSP 5.5.6	
	Does the Tribe or TGRA permit remote access for privileged functions only for compelling operational needs but document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system?	____	____	____	CSP 5.5.6	
	Is virtual escorting of privileged functions permitted only when all the following conditions are met:					
	1. The session shall be monitored at all times by an authorized escort?	____	____	____	CSP 5.5.6(1)	
	2. The escort shall be familiar with the system/area in which the work is being performed?	____	____	____	CSP 5.5.6(2)	

[4] A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.

[5] Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	3. The escort shall have the ability to end the session at any time?	____	____	____	CSP 5.5.6(3)	
	4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path?	____	____	____	CSP 5.5.6(4)	
	5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session[6].	____	____	____	CSP 5.5.6(5)	
12.	Based on inquiry and record examination, does the Tribe or TGRA authorize a personally owned information system to access, process, store or transmit CJI?	____	____	____	CSP 5.5.6.1	
	If yes, has the Tribe or TGRA established and documented the specific terms and conditions for personality owned information system usage?	____	____	____	CSP 5.5.6.1	
	When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices[7].					
13.	Based on inquiry and record examination, does the Tribe or TGRA allow publicly accessible computers[8] be used to access, process, store or transmit CJI?	____	____		CSP 5.5.6.2	
	This is not a permissible use.					

[6] This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.
[7] This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).
[8] Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.