#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.6	**Identification and Authentication**					
1.	Based on inquiry and record examination, does the Tribe or TGRA uniquely identify each person who is authorized to store, process, and/or transmit CJI/CHRI?	____	____	____	CSP 5.6.1	
	Based on inquiry and record examination, is a unique identification[1] required for all persons who administer and maintain the system(s) that access CJI/CHRI or networks leveraged for CJI/CHRI transit?	____	____	____	CSP 5.6.1	
	Based on inquiry and record examination, does the Tribe or TGRA require users to identify themselves uniquely before the user is allowed to perform any actions on the system?	____	____	____	CSP 5.6.1	
	Based on inquiry and record examination, does the Tribe or TGRA ensure that all user ID's belong to currently authorized users?	____	____	____	CSP 5.6.1	
	Based on inquiry and record examination, does the Tribe or TGRA maintain current identification data by adding new users and disabling and/or deleting former users?	____	____	____	CSP 5.6.1	
2.	Based on inquiry and record examination, does the Tribe or TGRA use an FBI authorized originating agency identifier[2] (ORI) in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction?	____	____	____	CSP 5.6.1.1	
3.	Based on inquiry and record examination, does the Tribe or TGRA authenticate[3] each individual's identity?	____	____	____	CSP 5.6.2	
	Based on inquiry and record examination, does the Tribe or TGRA include the authentication strategy as part of the audit for CSP compliance?	____	____	____	CSP 5.6.2	

[1] The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier.
[2] The original identifier between the requesting agency and the CSA shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.
[3] Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The Tribe or TGRA may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI/CHRI.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
4.	Based on inquiry and record examination, does the Tribe or TGRA allow users to use the same password[4] or PIN in the same logon sequence? If so, this is not permitted.	____	____	____	CSP 5.6.2.1	
5.	Based on inquiry and record examination, when a Tribe or TGRA elects to follow the basic password standards, are the passwords:					
	1. A minimum length of eight (8) characters on all systems?	____	____	____	CSP 5.6.2.1.1.1(1)	
	2. Not a dictionary word or proper name?	____	____	____	CSP 5.6.2.1.1.1(2)	
	3. Not the same as the User id?	____	____	____	CSP 5.6.2.1.1.1(3)	
	4. Expire within a maximum of 90 calendar days?	____	____	____	CSP 5.6.2.1.1.1(4)	
	5. Not identical to the previous ten (10) passwords?	____	____	____	CSP 5.6.2.1.1.1(5)	
	6. Not transmitted in the clear, outside the secure location?	____	____	____	CSP 5.6.2.1.1.1(6)	
	7. Not displayed when entered?	____	____	____	CSP 5.6.2.1.1.1(7)	
6.	Based on inquiry and record examination, when a Tribe or TGRA elects to follow the advanced password standards, did the Tribe or TGRA ensure:					
	1. Passwords are a minimum of twenty (20) characters in length with no additional complexity requirements imposed?[5]	____	____	____	CSP 5.6.2.1.1.2(1)	
	2. Password Verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing a password?	____	____	____	CSP 5.6.2.1.1.2(2)	
	3. Verifiers maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised?	____	____	____	CSP 5.6.2.1.1.2(3)	

[4] Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN).

[5] (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	For example, the list may include, but is not limited to:					
	a. Passwords obtained from previous breach corpuses?	____	____	____	CSP 5.6.2.1.1.2(3)(a)	
	b. Dictionary words?	____	____	____	CSP 5.6.2.1.1.2(3)(b)	
	c. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')?	____	____	____	CSP 5.6.2.1.1.2(3)(c)	
	d. Context-specific words, such as the name of the service, the username, and derivatives thereof?	____	____	____	CSP 5.6.2.1.1.2(3)(d)	
4.	When processing requests to establish and change passwords, do Verifiers compare the prospective passwords against the "banned passwords" list?	____	____	____	CSP 5.6.2.1.1.2(4)	
5.	If the chosen password is found to be part of a "banned passwords" list, does the Verifier:					
	a. Advise the user that they need to select a different password?	____	____	____	CSP 5.6.2.1.1.2(5)(a)	
	b. Provide the reason for rejection?	____	____	____	CSP 5.6.2.1.1.2(5)(b)	
	c. Require the user to choose a different password?	____	____	____	CSP 5.6.2.1.1.2(5)(c)	
6.	Do Verifiers limit the number of failed authentication attempts that can be made as described in CSP 5.5.3 Unsuccessful Login Attempts?	____	____	____	CSP 5.6.2.1.1.2(6)	
7.	Do Verifiers force a password change if there is evidence of authenticator compromise or every 365 days from the last password change?	____	____	____	CSP 5.6.2.1.1.2(7)	
8.	Do Verifiers use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks?	____	____	____	CSP 5.6.2.1.1.2(8)	
9.	Do Verifiers store passwords in a manner that is resistant to offline attacks by salting[6] and hashing[7] the password using a one-way key derivation[8] function when stored?	____	____	____	CSP 5.6.2.1.1.2(9)	

[6] The process of applying a non-secret value to data prior to applying a cryptographic process, such as hashing. This process changes the value to be hashed in a manner designed to ensure an attacker cannot reuse the results of computations for one instance.

[7] The process of applying a mathematical algorithm to data to produce an alphanumeric value (i.e. hash value) to be used as a representative of that data.

[8] Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	a. Are the salt at least 32 bits in length?	____	____	____	CSP 5.6.2.1.1.2(9)(a)	
	b. Is the salt chosen arbitrarily so as to minimize salt value collisions among stored hashes?	____	____	____	CSP 5.6.2.1.1.2(9)(b)	
	10. For each user, do Verifiers protect stored salt and resulting hash values using a password or PIN?	____	____	____	CSP 5.6.2.1.1.2(10)	
7.	Based on inquiry and record examination, when a Tribe or TGRA implement the use of a PIN as a standard authenticator, do the PIN attributes follow the guidance in CSP 5.6.2.1.1 Password?	____	____	____	CSP 5.6.2.1.2	
8.	Based on inquiry and record examination, does the Tribe or TGRA implement the use of an OTP[9] as an authenticator?	____	____	____	CSP 5.6.2.1.3	
	If yes, does the OTP meet the following requirements?					
	1. Be a minimum of six (6) randomly generated characters?	____	____	____	CSP 5.6.2.1.3(1)	
	2. Be valid for a single session?	____	____	____	CSP 5.6.2.1.3(2)	
	3. If not used, expire within a maximum of five (5) minutes after issuance?	____	____	____	CSP 5.6.2.1.3(3)	
9.	Based in inquiry and record examination does the Tribe or TGRA establish identifier and authenticator management processes?	____	____	____	CSP 5.6.3	
	Based on inquiry and record examination, does the Tribe or TGRA manage user identifiers as follows:					
	1. Uniquely identify each user?	____	____	____	CSP 5.6.3.1(1)	
	2. Verify the identity of each user?	____	____	____	CSP 5.6.3.1(2)	
	3. Receive authorization to issue a user identifier from an appropriate agency official?	____	____	____	CSP 5.6.3.1(3)	
	4. Issue the user identifier to the intended party?					
	5. Disable the user identifier after a specified period of inactivity?	____	____	____	CSP 5.6.3.1(4)	
	6. Archive user identifiers?	____	____	____	CSP 5.6.3.1(5)	
		____	____	____	CSP 5.6.3.1(6)	

[9] One-time passwords are considered a "something you have" token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
10.	Based on inquiry and record examination, does the Tribe or TGRA undertake the below in order to manage information system authenticators?[10]					
	1. Define initial authenticator content? 2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators?	____	____	____	CSP 5.6.3.2(1) CSP 5.6.3.2(2)	
	3. Change default authenticators upon information system installation?	____	____	____	CSP 5.6.3.2(3)	
	4. Change/refresh authenticators periodically?	____	____	____	CSP 5.6.3.2(4)	
11.	Based on inquiry and record examination, does the Tribe or TGRA ensure assertion mechanisms[11] used to communicate the results of a remote authentication to other parties are:					
	1. Digitally signed by a trusted entity (e.g., the identity provider)?	____	____	____	CSP 5.6.4(1)	
	2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion?	____	____	____	CSP 5.6.4(2)	
	Based on inquiry and record examination, does the Tribe or Tribe ensure assertions generated by a verifier expire after 12 hours and are not accepted thereafter by the relying party?	____	____	____	CSP 5.6.4	

[10] Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

[11] Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service.