#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.20	**Mobile devices**					
1.	Each Tribe or TGRA shall establish usage restrictions and implementation guidance for mobile devices; and authorize, monitor, control wireless access to systems which contain CJI/CHRI. Does the Tribe or TGRA have mobile devices with access to CJI/CHRI? Mobile devices include smartphones, tablets and laptop computers. Wireless technologies[1], in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. If yes, complete all questions. If no, the Tribe or TGRA is exempt from the requirements in CJISSECPOL Area 20.	____	____		CJISSECPOL 5.20	
2.	Has the Tribe or TGRA implemented the following controls for all tribal managed wireless access points with access to unencrypted CJI/CHRI: 1. Validation testing to ensure rogue APs (Access Points) do not exist in the 802.11[2] Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture?	____	____	____	CJISSECPOL 5.20.1.1(1)	
	2. Inventory of all Access Points (APs) and 802.11 wireless devices?	____	____	____	CJISSECPOL 5.20.1.1(2)	
	3. Physical security of APs to prevent unauthorized physical access and user manipulation?	____	____	____	CJISSECPOL 5.20.1.1(3)	
	4. AP boundary testing to determine the precise extent of the wireless coverage and to design the AP wireless coverage that limits the coverage area to only what is needed for operational purposes?	____	____	____	CJISSECPOL 5.20.1.1(4)	

[1] Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described in CJISSECPOL Policy Area 20.

[2] Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used in accordance with CJISSECPOL 5.20.1.1.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	5. Enabled user authentication and encryption mechanisms for the management interface of the AP?	____	____	____	CJISSECPOL 5.20.1.1(5)	
	6. The APs have strong administrative passwords and all passwords are changed in accordance with CJISSECPOL Identification and Authentication (IA)? See the related sample audit checklist at NIGC CJIS Resource Materials.	____	____	____	CJISSECPOL 5.20.1.1(6)	
	7. The reset function on APs is used only when needed and is only invoked by authorized personnel?	____	____	____	CJISSECPOL 5.20.1.1(7)	
	When the reset functions are used, the factory default settings are not utilized and the APs are restored to the latest security settings?	____	____	____	CJISSECPOL 5.20.1.1(7)	
	8. The default service set identifier (SSID) is changed in the APs?	____	____	____	CJISSECPOL 5.20.1.1(8)	
	The broadcast SSID feature has been disabled so the client SSID must match that of the AP?	____	____	____	CJISSECPOL 5.20.1.1(8)	
	The SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services?	____	____	____	CJISSECPOL 5.20.1.1(8)	
	9. All security features of the wireless product are enabled, including the cryptographic authentication, firewall, and other available privacy features?	____	____	____	CJISSECPOL 5.20.1.1(9)	
	10. The encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys?	____	____	____	CJISSECPOL 5.20.1.1(10)	
	11. The ad hoc mode has been disabled?	____	____	____	CJISSECPOL 5.20.1.1(11)	
	12. All nonessential management protocols are disabled on the APs?	____	____	____	CJISSECPOL 5.20.1.1(12)	
	13. All management access and authentication occurs via FIPS compliant secure protocols[3] (e.g. SFTP, HTTPS, SNMP over TLS, etc.)?	____	____	____	CJISSECPOL 5.20.1.1(13)	
	14. Logging (if supported) is enabled and the logs are reviewed on a recurring basis per local policy? At a minimum logs shall be reviewed monthly.	____	____	____	CJISSECPOL 5.20.1.1(14)	

[3] Disable non-FIPS compliant secure access to the management interface.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	15. The wireless network is insulated, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), from the operational wired infrastructure?	____	____	____	CJISSECPOL 5.20.1.1(15)	
	Access between wireless networks and the wired network is limited to only operational needs?	____	____	____	CJISSECPOL 5.20.1.1(15)	
	16. When disposing of APs that will no longer be used by the Tribe or TGRA, configuration settings are cleared to prevent disclosure of network configuration, keys, passwords, etc?	____	____	____	CJISSECPOL 5.20.1.1(16)	
3.	Certain internal functions on cellular devices[4] may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a "trusted" entity by the device. If a Tribe or TGRA allows managed devices to access CJI/CHRI outside the U.S., does the Tribe or TGRA perform a documented inspection to ensure all controls are in place and functioning properly in accordance with the Tribe's or TGRA's policies prior to and after deployment outside of the U.S? Any cellular device used to transmit CJI/CHRI via voice is exempt from the encryption and authentication requirements.	____	____	____	CJISSECPOL 5.20.1.2 CJISSECPOL 5.20.1.2.1 CJISSECPOL 5.20.1.2.2	
4.	If Bluetooth[5] is utilized, does the Tribe or TGRA implement security policies that dictate the use of Bluetooth and its associated devices based on the operational and business processes?	____	____	____	CJISSECPOL 5.20.1.3	

[4] Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and "aircards" are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

[5] Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.
Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications.

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
5.	Based on inquiry and record examination, if a Tribe or TGRA allow mobile devices that access or store CJI/CHRI to function as a Wi-Fi hotspot connecting to the Internet, are the mobile devices configured[6]:					
	1. To enable encryption on the hotspot[7]?	____	____	____	CJISSECPOL 5.20.1.4(1)	
	2. To ensure the hotspot SSID (required to change the hotspot's default SSID) does not identify the device make/model or Tribe/TGRA ownership?	____	____	____	CJISSECPOL 5.20.1.4(2)(a)	
	3. To create a wireless network password (Pre-shared key)[8]?	____	____	____	CJISSECPOL 5.20.1.4(3)	
	4. To enable the hotspot's port filtering/blocking features if present?	____	____	____	CJISSECPOL 5.20.1.4(4)	
	5. To only allow connections from the Tribe's or TGRA's controlled devices?	____	____	____	CJISSECPOL 5.20.1.4(5)	
6.	Based on inquiry and record examination, if a Tribe or TGRA allow wireless devices that access or store CJI/CHRI, does the Tribe/TGRA, at a minimum, ensure that wireless devices:					
	1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in System and Information Integrity (SI)? See the related sample audit checklist at NIGC CJIS Resource Materials.	____	____	____	CJISSECPOL 5.20.3(1)	
	2. Are configured for local device authentication (see CJISSECPOL Section 5.20.7.1)?	____	____	____	CJISSECPOL 5.20.3(2)	
	3. Use advanced authentication or NIGC CSA CSO approved compensating controls (see CJISSECPOL 5.20.7.2.1)?	____	____	____	CJISSECPOL 5.20.3(3)	
	4. Encrypt all CJI/CHRI resident on the device?	____	____	____	CJISSECPOL 5.20.3(4)	
	5. Erase cached information, to include authenticators (see Identification and Authentication (IA))[9] in applications, when session is terminated?	____	____	____	CJISSECPOL 5.20.3(5)	

[6] Refer to the requirements in CJISSECPOL Section 5.20.1.2 encryption for item #1. Refer to the requirements in Access Control (AC). Password for item #3. Only password attributes #1, #2 and #3 are required or have an MDM solution to provide the same security as identified in items 1 – 5 above.

[7] Refer to the requirements in Systems and Communications Protection (SC) encryption for item #1. See the related sample audit checklist at NIGC CJIS Resource Materials.

[8] Refer to the requirements in Identification and Authentication (IA) for item #3. See the related sample audit checklist at NIGC CJIS Resource Materials.

[9] See the related sample audit checklist at NIGC CJIS Resource Materials.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management[10] (MDM) system that facilitates the ability to provide firewall services from the tribal level?	____	____	____	CJISSECPOL 5.20.3(6)	
	7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the tribal level?	____	____	____	CJISSECPOL 5.20.3(7)	
7.	In many cases, CJISSECPOL requirements cannot be met with a mobile device without the installation of a third-party MDM, application, or supporting service infrastructure. Based on inquiry and record examination, does the Tribe/TGRA have a third-party MDM, application, or supporting service infrastructure?	____	____	____	CJISSECPOL 5.20.4	
8.	Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching. Based on inquiry and record examination, does the Tribe/TGRA monitor mobile devices to ensure their patch and update state is current?	____	____	____	CJISSECPOL 5.20.4.1	

[10] Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
9.	A personal firewall[11] shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). Based on inquiry and record examination, does the personal firewall[12] perform the following activities:					
	1. Manage program access to the Internet?	____	____	____	CJISSECPOL 5.20.4.3(1)	
	2. Block unsolicited requests to connect to the user device?	____	____	____	CJISSECPOL 5.20.4.3(2)	
	3. Filter incoming traffic by IP address or protocol?	____	____	____	CJISSECPOL 5.20.4.3(3)	
	4. Filter incoming traffic by destination ports?	____	____	____	CJISSECPOL 5.20.4.3(4)	
	5. Maintain an IP traffic log?	____	____	____	CJISSECPOL 5.20.4.3(5)	
10.	In addition to the CJISSECPOL requirements for Incident Response[13], a Tribe or TGRA shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. Based on inquiry and record examination, does the Tribe or TGRA implement reporting procedures for the following situations:					
	1. Loss of device control:					
	a. Device known to be locked, minimal duration of loss?	____	____	____	CJISSECPOL 5.20.5(1)(a)	
	b. Device lock state unknown, minimal duration of loss?	____	____	____	CJISSECPOL 5.20.5(1)(b)	
	c. Device lock state unknown, extended duration of loss?	____	____	____	CJISSECPOL 5.205(1)(c)	
	d. Device known to be unlocked, more than momentary duration of loss?	____	____	___	CJISSECPOL 5.20.5(1)(d)	

[11] Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

[12] Mobile devices with limited-feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full-feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

[13] See the related sample audit checklist at NIGC CJIS Resource Materials.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	2. Total loss of device?	____	____	____	CJISSECPOL 5.20.5(2)	
	3. Device compromise?	____	____	____	CJISSECPOL 5.20.5(3)	
	4. Device loss or compromise outside the United States?	____	____	____	CJISSECPOL 5.20.5(4)	
11.	Multiple user accounts are not generally supported on limited-feature mobile operating systems[14]. Access control shall be accomplished by the application that accesses CJI.					
	Based on inquiry and record examination does the limited-feature mobile operating system(s) and application(s) comply with CJIS requirements for Access Control[15]?	____	____	____	CJISSECPOL 5.20.6 CJISSECPOL 5.20.7	
12.	Based on inquiry and record examination, does the local device authentication require each device be unlocked before device use?	____	____	____	CJISSECPOL 5.20.7.1	
	If a Tribe or TGRA allow wireless devices that access or store CJI/CHRI, does the authenticator used meet the requirements in Identification and Authentication (IA)[16]?	____	____	____	CJISSECPOL 5.20.7.1	

[14] Due to the technical methods used for identification and authentication on many limited-feature mobile operating systems, achieving compliance may require many different components.
[15] See the related sample audit checklist at NIGC CJIS Resource Materials.
[16] See the related sample audit checklist at NIGC CJIS Resource Materials.