#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	Media Protection (MP)					
1.	Does the Tribe or TGRA develop, document, and disseminate to authorized individuals an agency-level media protection policy[1] that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance?	____	____	____	MP-1, a.1(a)	
	Is the policy consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	____	____	____	MP-1, a.1.(b)	
	For the questions above, simply restating controls does not constitute an organizational policy or procedure.					
2.	Does the Tribe or TGRA develop, document, and disseminate to authorized individuals procedures[2] to facilitate the implementation of the media protection policy and the associated media protection controls?	____	____	____	MP-1, a.2	
3.	Has the Tribe or TGRA designated an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures?	____	____	____	MP-1, b	
4.	Based on inquiry and record examination, does the Tribe or TGRA review and update the media protection policy and procedures annually and following any security incidents involving digital[3] and/or non-digital media[4]?	____	____	____	MP-1, c.1.2	
5.	Based on inquiry and record examination, does the Tribe or TGRA restrict access to digital and non-digital media to authorized individuals?	____	____	____	MP-2	

[1] The policy can be included as part of the general security and privacy policy or comprise multiple policies.
[2] Procedures describe how the policy or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.
[3] Digital Media – Any form of electronic media designed to store data in a digital format. This includes but is not limited to: memory device in laptops, computers, and mobile devices and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.
[4] Non-digital Media – Non-digital media means a hard copy or physical representation of information, including, but not limited to, paper copies, printer ribbons, drums, microfilm, platens, and other forms of preserved or preservable information.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
6.	Does the Tribe or TGRA exempt digital and non-digital media containing CHRI from marking if the media remains within a physically secure location or controlled areas?	____	____	____	MP-3, b	
7.	Based on inquiry and record examination, does the Tribe or TGRA physically control[5] and securely store[6] digital and non-digital media within physically secure locations or controlled areas[7] and encrypt CJI on digital media when physical and personnel restrictions are not feasible?	____	____	____	MP-4, a	
8.	Does the Tribe or TGRA protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures?	____	____	____	MP-4, b	
9.	Based on inquiry and record examination, does the Tribe or TGRA protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption, as defined in CSP 5.10.1.2?	____	____	____	MP-5, a	
	If yes, does the Tribe or TGRA protect physical media at the same level as the information is protected in electronic form?	____	____	____	MP-5, a	
10.	Does the Tribe or TGRA restrict the activities associated with transport of electronic and physical media to authorized personnel[8]?	____	____	____	MP-5, a	
11.	Does the Tribe or TGRA maintain accountability[9] for system media during transport outside of the physically secure location or controlled areas?	____	____	____	MP-5, b	

[5] Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to access and return media, and maintaining accountability for stored media.
[6] Secure storage includes a locked drawer, desk, or cabinet or a controlled media library.
[7] Controlled areas are spaces that provide physical and procedural controls to meet established requirements for protecting information and systems.
[8] Authorized transport and courier personnel may include individuals external to the agency.
[9] Maintaining accountability of media during transport includes restricting transport to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
12.	Does the Tribe or TGRA document activities associated with the transport of system media?	____	____	____	MP-5, c	
13.	Does the Tribe or TGRA restrict the activities associated with the transport of system media to authorized personnel[10]?	____	____	____	MP-5, d	
14.	Based on inquiry and record examination, does the Tribe or TGRA sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals[11]?	____	____	____	MP-6, a	
15.	Based on inquiry and record examination, does the Tribe or TGRA employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information?	____	____	____	MP-6, b	
16.	Based on record examination, does the Tribe or TGRA restrict the use of digital and non-digital media on agency owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical[12], physical[13], or administrative controls[14]?	____	____	____	MP-7, a	

[10] *See* note 10, *supra.*

[11] Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration.

[12] Examples of technical controls: port disabling, access control lists (ACL), security groups, group policy objects (GPO), mobile device management (MDM).

[13] Example of physical control: locked server cage, disconnect CD-ROM drive in PC, remove USB port.

[14] Example of administrative controls: the agency's electronic media policy defining how flash drives are to be used within the agency rules of behavior.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
17.	Based on inquiry and record examination, does the Tribe or TGRA prohibit the use of personally owned digital media devices[15] on all agency owned or controlled systems that store, process, or transmit criminal justice information?	____	____	____	MP-7, b	
18.	Based on inquiry and record examination, does the Tribe or TGRA prohibit the use of digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner?	____	____	____	MP-7, c	

[15] Such as mobile devices/phones with information storage capabilities.