#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.3	**Incident Response**					
1.	To ensure protection of CJI/CHRI, has the Tribe or TGRA established operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities?	____	____	____	CSP 5.3(i)	
	To ensure protection of CJI/CHRI, does the Tribe or TGRA track, document, and report incidents to their LASO and NIGC ISO?	____	____	____	CSP 5.3(ii)	
2.	The Tribe or TGRA shall promptly report incident information to their LASO and NIGC ISO. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. This obligation applies to all employees and contractors. Does the Tribe or TGRA have formal event reporting and escalation procedures[1] in place?	____	____	____	CSP 5.3.1	
	If the Tribe or TGRA has outsourced noncriminal justice administrative functions to a Contractor, verify that the reporting and escalation procedures comply with the associated requirements in the Security and Management Control Outsourcing Standard for Non-Channelers[2], as identified in the Sample 90 day audit checklist for Contractor access to FBI CHRI from the NIGC[3].	____	____	____	OS 2.08 OS 8.01(c) OS 8.01(d) OS 9.03	
3.	Does the Tribe or TGRA have procedures in place to handle security events and weaknesses effectively once they have been reported[4] to the NIGC ISO (iso@nigc.gov)?	____	____	____	CSP 5.3.2	

[1] All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the LASO and or designated point of contact and the NIGC ISO (iso@nigc.gov).

[2] https://www.fbi.gov/file-repository/compact-council-security-and-management-control-outsourcing-standard-for-non-channelers.pdf/view

[3] https://www.nigc.gov/images/uploads/Sample_90_day_audit_checklist_for_contractor_access_to_FBI_CHRI_from_the_NIGC_Final.pdf

[4] The sample security incident response form from CJIS_Security_Policy_v5-9_20200601 can be located at https://www.nigc.gov/compliance/CJIS-Training-Materials

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
4.	Has the Tribe or TGRA implemented an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery? Wherever feasible, the Tribe or TGRA shall employ automated mechanisms to support the incident handling process.	____	____	____	CSP 5.3.2.1	
5.	Does the Tribe/TGRA obtain incident related information from a variety of sources including, but not limited to: 1. Audit monitoring? 2. Network monitoring? 3. Physical access monitoring? 4. User/administrator reports?	 ____ ____ ____ ____	 ____ ____ ____ ____	 ____ ____ ____ ____	CSP 5.3.2.1	
6.	Does the Tribe/TGRA incorporate lessons learned from ongoing incident handling activities into the incident response procedures and implement procedures accordingly?	____	____	____	CSP 5.3.2.1	
7.	Does the Tribe or TGRA have a process to collect, retain and present evidence of information security incidents for follow-up action against a person or agency for purposes of a legal action, if necessary?	____	____	____	CSP 5.3.2.2	
8.	Does the Tribe or TGRA ensure general incident response roles and responsibilities are included as part of required security awareness training?	____	____	____	CSP 5.3.3	
9.	Does the Tribe or TGRA track and document security incidents on an ongoing basis?	____	____	____	CSP 5.3.4	
10.	Refer to CSP 5.13.5 for additional incident response requirements related to mobile devices.				CSP 5.13.5	