Part 10, Chapter 3: Manual Exhibit 10-3-A

Indian Health Service
Cybersecurity and Privacy Control Definitions
Audit and Accountability Controls

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," provides a catalog of security and privacy controls and control enhancements that must be implemented for Federal information systems.

Many of these controls and enhancements include specific parameters that must be defined by federal agencies. The Department of Health and Human Services (HHS) has defined roughly 50 percent of these parameters in the HHS Office of the Chief Information Officer Policy for Information Systems Security and Privacy (IS2P). HHS directs Operating Divisions to inherit these parameters and develop their own definitions for the remaining 50 percent.

The Indian Health Service (IHS) Cybersecurity and Privacy Control Definitions (CPCD) specifies the IHS-defined security control parameters in compliance with HHS direction. The Federal Risk and Authorization Management Program (FedRAMP) parameters, specifically applicable to cloud systems, are located at https://www.fedramp.gov/documents/.

The NIST SP 800-53, Rev 4 Audit and Accountability (AU) family controls that were withdrawn or were not selected by HHS are not included in the table below. The NIST SP 800-53, Rev 4 controls are located at https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

Audit and Accountability (AU)			**IHS Minimum Requirement by System Category**		
Control ID	**Control Title**	**Control Description**	**Low**	**Moderate**	**High**
AU-1	Audit and Accountability Policy and Procedures	IHS: a. Develops, documents, and disseminates to all IHS personnel (via ihs.gov websites) for IHS-wide policies/procedures and to all system personnel for individual systems as required by the System Owner or designee: 1. An Audit and Accountability (AU) policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance (*Note: IHS covers this control by establishing the Indian Health Manual (IHM), Part 10, Cybersecurity*); and 2. Procedures to facilitate the implementation of the AU policy and associated AU controls. b. Per IHM Part 1, Chapter 1, "Indian Health Service Manual System," reviews the AU policy at least every two years and submits to the Division of Regulatory and Policy Coordination (DRPC) for revision when needed. c. Reviews the AU procedures at least every three years and updates the procedures when needed.	Selected	Selected	Selected

AU-2	Audit Events	The System Owner or designee: a. Determines that the information system is capable of auditing the following events: • Server alerts and error messages • User log-on and log-off (successful or unsuccessful) • System administration activities • Modification of privileges and access • Start up and shut down • Modifications to the application • Application alerts and error messages • Configuration changes • Account creation, modification, or deletion • (Moderate and High only) Read access to sensitive information • (Moderate and High only) Modification to sensitive information • (Moderate and High only) Printing sensitive information • Applications invoked • (High only) Addition, modification, and/or deletion of sensitive information b. Coordinates the security audit function with other organizational entities requiring audit-related information, to enhance mutual support and to help guide the selection of auditable events.	Selected	Selected	Selected

AU-2 (continued)	Audit Events	c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents. d. Determines that the following events are to be audited within the information system at least weekly: • Unsuccessful log-on attempts that result in a locked account/node • Configuration changes • Application alerts and error messages • System administration activities • Modification of privileges and access • Account creation, modification, or deletion *Note: These are the minimum set of events that should be audited, but IHS System Owners or applicable organization components are free to expand this list if desired based on organizational risk.*	Selected	Selected	Selected
AU-2 c.e.3	Reviews and Updates	IHS reviews and updates the list of audited events annually and whenever there is a significant system modification.	Not Selected	Selected	Selected

AU-3	Content of Audit Records	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	Selected	Selected	Selected
AU-3 c.e.1	Additional Audit Information	The information system generates, if applicable, audit records containing the following additional information: • Name of the accessed file • Program or command used to initiate the event • Source and destination addresses	Not Selected	Selected	Selected
AU-3 c.e.2	Centralized Management of Planned Audit Record Content	The information system provides centralized management and configuration of the content captured in audit records, and all records must be fed into the IHS's centralized audit record management tool.	Not Selected	Not Selected	Selected
AU-4	Audit Storage Capacity	IHS allocates audit record storage capacity. Adequate storage capacity to support storing of audit records is defined by National Archives and Records Administration (NARA) General Records Schedule (GRS) GRS 3.2, Information Systems Security Records and GRS 4.2 Information Access and Protection Records.	Selected	Selected	Selected

AU-5	Response to Audit Processing Failures	The information system: a. Alerts the System Owner, and/or others designated by the System Owner in the event of an audit processing failure; and b. In the case of security audit log processing failure, information system processing must be investigated for mitigation (for Moderate and High only).	Selected	Selected	Selected
AU-5 c.e.1	Audit Storage Capacity	The information system provides a warning to the System Owner, and/or others designated by the System Owner immediately when allocated audit record storage volume reaches 80-85 percent.	Not Selected	Not Selected	Selected
AU-5 c.e.2	Real-Time Alerts	The information system provides real time alerts, instantly to the System Owner and/or others designated by the System Owner when the following audit failure events occur: • Three failed log-on attempts • Unauthorized modification of system files.	Not Selected	Not Selected	Selected
AU-6	Audit Review, Analysis, and Reporting	IHS: a. Reviews and analyzes information system audit records weekly for indications of inappropriate or unusual activity; and b. Reports findings to the System Owner, and/or others designated by the System Owner.	Selected	Selected	Selected
AU-6 c.e.1	Process Integration	IHS employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	Not Selected	Selected	Selected

AU-6 c.e.3	Correlate Audit Repositories	IHS analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	Not Selected	Selected	Selected
AU-6 c.e.5	Integration/ Scanning and Monitoring Capabilities	IHS integrates analysis of audit records with analysis of data collected from other sources, such as vulnerability scanning information, performance data, and information system monitoring information, to further enhance the ability to identify inappropriate or unusual activity.	Not Selected	Not Selected	Selected
AU-6 c.e.6	Correlation with Physical Monitoring	IHS correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	Not Selected	Not Selected	Selected
AU-7	Audit Reduction and Report Generation	The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.	Not Selected	Selected	Selected

AU-7 c.e.1	Automatic Processing	The information system provides the capability to process audit records for events of interest based on User ID, event time/date stamp, IP/MAC address, type of event, and event outcome. *Note: Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals; event types; event locations; event times; event dates; system resources involved; IP addresses involved; or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.*	Not Selected	Selected	Selected
AU-8	Time Stamps	The information system: a. Uses encrypted Network Time Protocol (NTP) servers to generate time stamps for audit records; and b. Records time stamps for audit records that can be expressed in Coordinated Universal Time or Greenwich Mean Time.	Selected	Selected	Selected

AU-8 c.e.1	Synchronization with Authoritative Time Source	The information system: a. Compares the internal information system clocks at least weekly with the federally-maintained NTP stratum at http://tycho.usno.navy.mil/ntp.html; and b. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than one minute.	Not Selected	Selected	Selected
AU-9	Protection of Audit Information	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Selected	Selected	Selected
AU-9 c.e.2	Audit Backup on Separate Physical Systems/ Components	The information system backs up audit records daily onto a physically different system or system component than the system or component being audited.	Not Selected	Not Selected	Selected
AU-9 c.e.3	Cryptographic Protection	The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.	Not Selected	Not Selected	Selected
AU-9 c.e.4	Access by Subset of Privileged Users	IHS authorizes access to management of audit functionality to only the System Owner and/or others designated by the System Owner.	Not Selected	Selected	Selected

AU-10	Non-Repudiation	The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed account creation/modification, system shutdown, data modification, deletion, or location change. *Note: Non-repudiation provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, or receiving a message. For example: the use of PIV cards to digitally sign information is a common control that provides significant protection against repudiation.*	Not Selected	Not Selected	Selected
AU-11	Audit Record Retention	IHS employs audit record retention requirements as defined by NARA GRS 3.2, "Information Systems Security Records," and GRS 4.2, "Information Access and Protection Records," to ensure that long-term audit records generated by the information system can be retrieved.	Selected	Selected	Selected
AU-12	Audit Generation	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 (d) for the information system components identified by the IHS; b. Allows System Owner, and/or others designated by System Owner, to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 (d) with the content defined in AU-3.	Selected	Selected	Selected

AU-12 c.e.1	Time-Correlated Audit Trail	The information system compiles audit records from all system and network components including server/hosts, firewalls, routers, load balancers, etc. into a system-wide (logical or physical) audit trail that is time-correlated to within +/- five minutes.	Not Selected	Not Selected	Selected
AU-12 c.e.3	Changes by Authorized Individuals	The information system provides the capability for designated personnel to change the auditing to be performed on any IHS information system component based on changes to information technologies or threats to IHS within any timeframe deemed acceptable by the Chief Information Security Officer at the time of the change.	Not Selected	Not Selected	Selected