EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

August 27, 2021

M-21-31

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

Recent events, including the SolarWinds incident, underscore the importance of increased government visibility before, during, and after a cybersecurity incident. Information from logs on Federal information systems[1] (for both on-premises systems and connections hosted by third parties, such as cloud services providers (CSPs)) is invaluable in the detection, investigation, and remediation of cyber threats.

Executive Order 14028, *Improving the Nation's Cybersecurity*,[2] directs decisive action to improve the Federal Government's investigative and remediation capabilities. This memorandum was developed in accordance with and addresses the requirements in section 8 of the Executive Order for logging, log retention, and log management, with a focus on ensuring centralized access and visibility for the highest-level enterprise security operations center (SOC) of each agency. In addition, this memorandum establishes requirements for agencies[3] to increase the sharing of such information, as needed and appropriate, to accelerate incident response efforts and to enable more effective defense of Federal information and executive branch departments and agencies.

Section I: Maturity Model for Event Log Management

This memo establishes a maturity model to guide the implementation of requirements across four Event Logging (EL) tiers, as described in Table 1 below.

[1] As used in this memorandum, "Federal information system" has the meaning given in Executive Order 14028.
[2] Available at https://www.federalregister.gov/d/2021-10460
[3] As used in this memorandum, "agency" has the meaning given in 44 U.S.C. § 3502. The requirements established by this memorandum do not apply to national security systems, as defined in Executive Order 14028.

Table 1: Summary of Event Logging Tiers

Event Logging Tiers	Rating	Description
EL0	Not Effective	Logging requirements of highest criticality are either not met or are only partially met
EL1	Basic	Only logging requirements of highest criticality are met
EL2	Intermediate	Logging requirements of highest and intermediate criticality are met
EL3	Advanced	Logging requirements at all criticality levels are met

These tiers will help agencies prioritize their efforts and resources so that, over time, they will achieve full compliance with requirements for implementation, log categories, and centralized access. Agencies should also prioritize their compliance activities by focusing first on high-impact systems and high value assets (HVAs).

Tier EL0, Rating – Not Effective

The agency or one or more of its components have **not** implemented the following requirement:

- Ensuring that the Required Logs categorized as Criticality Level 0 are retained in acceptable formats for specified timeframes, per technical details described in Appendix C (*Logging Requirements – Technical Details*).

Tier EL1, Rating – Basic

The agency and all of its components meet the following requirements, as detailed in Table 2 (*EL1 Basic Requirements*) within Appendix A (*Implementation and Centralized Access Requirements*):

- Basic Logging Categories
- Minimum Logging Data
- Time Standard
- Event Forwarding
- Protecting and Validating Log Information
- Passive DNS
- Cybersecurity Infrastructure Security Agency (CISA) and Federal Bureau of Investigations (FBI) Access Requirements
- Logging Orchestration, Automation, and Response – Planning
- User Behavior Monitoring – Planning
- Basic Centralized Access

Tier EL2, Rating – Intermediate

The agency and all of its components meet the following requirements, as detailed in Table 3 (*EL2 Intermediate Requirements*) within Appendix A (*Implementation and Centralized Access Requirements*):

- Meeting EL1 maturity level
- Intermediate Logging Categories
- Publication of Standardized Log Structure
- Inspection of Encrypted Data
- Intermediate Centralized Access

Tier EL3, Rating – Advanced

The agency and all its components meet the following requirements, as detailed in in Table 4 (*EL3 Advanced Requirements*) within Appendix A (*Implementation and Centralized Access Requirements*):

- Meeting EL2 maturity level
- Advanced Logging Categories
- Logging Orchestration, Automation, and Response – Finalizing Implementation
- User Behavior Monitoring – Finalizing Implementation
- Application Container Security, Operations, and Management
- Advanced Centralized Access

Section II: Agency Implementation Requirements

Agencies must immediately begin efforts to increase performance in accordance with the requirements of this memorandum. Specifically, agencies must:

- Within 60 calendar days of the date of this memorandum, assess their maturity against the maturity model in this memorandum and identify resourcing and implementation gaps associated with completing each of the requirements listed below. Agencies will provide their plans and estimates to their OMB Resource Management Office (RMO) and Office of the Federal Chief Information Officer (OFCIO) desk officer.
- Within one year of the date of this memorandum, reach EL1 maturity.
- Within 18 months of the date of this memorandum, achieve EL2 maturity.
- Within two years of the date of this memorandum, achieve EL3 maturity.
- Provide, upon request and to the extent consistent with applicable law, relevant logs to the Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI). This sharing of information is critical to defend Federal information systems.
- Share log information, as needed and appropriate, with other Federal agencies to address cybersecurity risks or incidents.

Section III: Government-Wide Responsibilities

The following agencies bear specialized responsibilities as part of government-wide efforts to improve the management and use of logging practices:

CISA is responsible for the following actions:

- Deploying teams to advise agencies in their assessment of logging capabilities.
- Developing and publishing tools, in coordination with the FBI, to help agencies facilitate their assessment of logging maturity across the organization.

The Department of Commerce is responsible for the following actions:

- Continuing to maintain National Institute of Standards and Technology (NIST) Special Publication (SP) 800-92,[4] *Guide to Computer Security Log Management*, in coordination with CISA and the FBI.
- Incorporating the requirements of this memorandum regarding logging, log retention, and log management in the next revision of SP 800-92 and other relevant publications.

Section IV: Policy Assistance

Address all questions or inquiries regarding this memorandum to the OMB Office of the Federal Chief Information Officer (OFCIO) via email: ofcio@omb.eop.gov.

Attachments

Appendix A: Implementation and Centralized Access Requirements

Appendix B: Definitions

Appendix C: Logging Requirements – Technical Details

[4] Available at https://csrc.nist.gov/publications/detail/sp/800-92/final

Appendix A: Implementation and Centralized Access Requirements

Table 2: EL1 Basic Requirements

Basic Logging Categories	Ensuring that Required Logs categorized as Criticality Level 0 are retained in acceptable formats for specified timeframes, per technical details described in Appendix C.
Minimum Logging Data	At a minimum, agencies shall ensure that each event log contains the following data, if applicable: • Properly formatted and accurate timestamp (see below for Time Standard Requirements) • Status code for the event type • Device identifier (MAC address[5] or other unique identifier) • Session / Transaction ID • Autonomous System Number • Source IP (IPv4) • Source IP (IPv6) • Destination IP (IPv4) • Destination IP (IPv6) • Status Code • Response Time • Additional headers (i.e., HTTP headers) • Where appropriate, the username and/or userID shall be included • Where appropriate, the command executed shall be included • Where possible, all data shall be formatted as key-value-pairs allowing for easy extraction • Where possible, a unique event identifier shall be included for event correlation; a unique event identifier shall be defined per event type[6]

[5] Agencies should configure all hosts to have MAC randomization turned off. Where possible, this configuration should be maintained automatically.

[6] Software developed by agencies or by contractors on behalf of agencies must log unique event identifiers for each event in accordance with these requirements.

Time Standard	Consistent timestamp formats across all event logs are necessary for accurate and efficient event correlation and log analysis. Timestamps must be applied consistently to logs from all computing devices, routers, switches, and servers. Agencies shall maintain log timestamps in a format that meets the following requirements, based on both ISO 8601 and RFC 3339: Date and Time on the Internet: Timestamps.[7] • YYYY-MM-DDThh:mm:ss.mmmZ (Zulu time, UTC+0) and • YYYY-MM-DDThh:mm:ss.mmm+04:00 (UTC+4) • YYYY = four-digit year • MM = two-digit month • DD = two-digit day of the month • T = a set character indicating the start of the time element • hh = two digits of an hour (00 through 23) • mm = two digits of a minute • ss = two digits of a second • mmm = three digits of a millisecond (000 through 999) • +|- = time zone designator (Z or +hh:mm or -hh:mm), the + or – values indicate how far ahead or behind a time zone is from the UTC (Coordinated Universal Time) zone. Agencies shall use a GPS master station clock as a baseline reference for timestamps used for logs and systems producing logs. If GPS reference is not possible, agencies shall use NIST's authenticated time service.[8] Public, unauthenticated, and unencrypted NTP pools shall only be used as an option of last resort, and only for as long as needed to begin leveraging other options.
Event Forwarding	Event Forwarding allows administrators to obtain events from remote computers, also called source computers or forwarding computers, and store them on a central server known as the collector computer. Agencies shall forward all required logging data, in near real- time[9] and on an automated basis, to centralized systems responsible for security, information, and event monitoring (SIEM); bulk storage; and other

[7] Software developed by agencies or by contractors on behalf of agencies must log timestamps for each event in accordance with these requirements. If the software does not produce data in this format, Federal agencies will transform records to conform to these standards before the data is ingested into the SIEM or stored in bulk storage.
[8] https://www.nist.gov/pml/time-and-frequency-division/time-services/nist-authenticated-ntp-service
[9] The term "near real-time" or "nearly real-time" (NRT) refers to the time delay introduced by automated data processing or network transmission between the occurrence of an event and the use of the processed data, such as for display or feedback and control purposes.

	analytical workflows or services. Data must be encrypted in transit between its source and destination. Agencies must ensure the original log can be replayed for future use.

Protecting and Validating Log Information	To ensure data integrity, logging facilities and log information must be protected by cryptographic methods from tampering and unauthorized access. Agencies shall protect and monitor the integrity of their logs and systems producing logs by:
	• Verifying that event logging is enabled and active for system components.
	  ○ Traps shall be put in place to monitor these data streams for disruption.
	  ○ These traps shall be monitored.
	• Ensuring that only individuals who have a job-related need can view, access, or modify log files.
	• Documenting views and usage of log files and regularly reviewing/auditing the resulting records.
	• Confirming that current log files are protected from unauthorized modifications via access control mechanisms, such as virtual or physical segregation.
	• Ensuring that current log files are promptly backed up to an authorized source, such as a centralized log server or write-once media.
	• Using integrity-verification mechanisms to detect unauthorized changes to event logging configuration and log files that are no longer being written to or are considered closed.
	• Conducting integrity checks periodically and upon access against the log hashes throughout their retention period.
	• When logging stops unexpectedly, audit alerts shall be sent in near real-time to any parties responsible for monitoring. The responsible party must promptly investigate the cause of the disruption and take appropriate corrective actions.
	• Monitoring across the enterprise for unexpected changes to files or configuration items, including changes to:
	  ○ Credentials
	  ○ Privileges and security settings
	  ○ Content
	  ○ Core attributes and size
	  ○ Hash values
	  ○ Configuration values

Passive DNS	Federal agencies shall implement a Domain Name System (DNS) logging system that meets the requirements identified in Appendix C, including DNS requests made over encrypted DNS connections. Agencies shall implement accompanying analytics that allow for rapid identification of the host that sourced each DNS query. This capability

	shall be monitored and triaged. Federal agencies shall automate the production of a list of hostnames that are frequently accessed or looked up by legitimate users within their agency, but are not included in general top domain lists identified by CISA or available publicly or via subscription. Agencies should make that list automatically accessible to CISA or submit it to CISA daily via an acceptable automated mechanism.
CISA and FBI Access Requirements	Agencies shall provide logs and other relevant data to CISA and the FBI upon request, to the extent consistent with applicable law, including 44 U.S.C. § 3553(l). Agencies shall provide such data in a format and by means agreed upon by the agency, CISA, or the FBI, and shall do so pursuant to timelines specified by CISA or the FBI. Those timelines may require near real-time access to data.
Logging Orchestration, Automation, and Response – Planning	Federal agencies shall maintain and manage logs by leveraging the additional logging to develop automated hunt and incident response playbooks. Such playbooks shall take advantage of Security, Orchestration, Automation, and Response (SOAR) capabilities. Agencies at EL1 stage shall start planning on how to best implement SOAR capabilities in their environment. For additional implementation requirements, please see Table 4, *EL3 Advanced Requirements, Logging Orchestration, Automation, and Response – Finalizing Implementation*.
User Behavior Monitoring – Planning	User behavioral analytics allow for early detection of malicious behavior. This technology leverages machine learning and artificial intelligence techniques to detect anomalous user actions and help combat advanced threats. Agencies at EL1 stage shall start planning on how to best implement a user behavior analytics capability in their environment, leveraging the logging requirements, in order identify potentially malicious or malicious activity. Agencies are expected to finalize their implementation of this capability to achieve EL3 maturity level. For additional implementation requirements, please see Table 4, *EL3 Advanced Requirements, User Behavior Monitoring – Finalizing Implementation*.
Basic Centralized Access	Logs should be centrally aggregated by an agency component-level Enterprise Log Manager (ELM). Traps for detecting data-stream disruption should be monitored by the component-level SOC. The DNS logging system and accompanying analytics shall be monitored and triaged by the component-level SOC.

Table 3: EL2 Intermediate Requirements

EL1 maturity level	All requirements for EL1 must be met.
Intermediate Logging Categories	Required Logs categorized as Criticality Level 1 and 2 must be retained in acceptable formats for specified timeframes, per technical details described in Appendix C.
Publication of Standardized Log Structure	For all software developed by or on behalf of Federal agencies that produces logs and is deployed in Federal environments, Federal agencies shall provide a document detailing the structure (schema) for those logs to CISA. Agencies shall refer to guidance from CISA in developing this documented schema. Federal agencies shall also provide all updates to the schema to CISA no later than one business day after they are finalized. The schema and associated documentation shall be published to Data.gov.
Inspection of Encrypted Data	Federal agencies shall retain and store in cleartext form the data or metadata from Appendix C that is collected in their environment. If agencies perform full traffic inspection through active proxies, they should log additional available fields as described in Appendix C and can work with CISA to implement these capabilities. If agencies do not perform full traffic inspection, they should log the metadata available to them. In general, agencies are expected to follow zero-trust principles concerning least privilege and reduced attack surface, and relevant guidance from OMB and CISA relating to zero-trust architecture.
Intermediate Centralized Access	Required Logs categorized as Criticality Levels 0 and 1 are accessible and visible for the highest-level security operations at the head of each agency. Required Logs categorized as Criticality Levels 2 are retained, at a minimum, at component level. • Traps for detecting data-stream disruption should be monitored by the component-level and top-level enterprise SOCs. The DNS logging system and accompanying analytics shall be monitored and triaged by the component-level and top-level enterprise SOCs. The enterprise SOC shall ensure that cross-organizational analytics are established for use across agency components.

Table 4: EL3 Advanced Requirements

EL2 maturity level	All requirements for EL2 must be met.
Advanced Logging Categories	Required Logs categorized as Criticality Level 3 must be retained in acceptable formats for specified timeframes, per technical details described in Appendix C.
Logging Orchestration,	Agencies shall finalize and implement automated hunt and incident response playbooks. Federal agencies shall also provide any updates to

Automation, and Response – Finalizing Implementation	the playbooks and automation integrations to CISA no later than one business day after they are finalized.
User Behavior Monitoring – Finalizing Implementation	User behavioral analytics must be implemented in order to allow for early detection of malicious behavior. This technology leverages machine learning and artificial intelligence techniques to detect anomalous user actions and help combat advanced threats. Agencies shall implement a user behavior analytics capability, leveraging the logging requirements, in order identify potentially malicious or malicious activity. This capability shall monitor all user and non-user accounts. This capability shall be monitored and triaged by component- and top-level agency Security Operations Centers (SOC). At a minimum, user Behavior Monitoring should be configured to detect and alert on: • Compromised user credentials • Privileged-user compromise • Improper asset access • Compromised system/host/device • Lateral movement of threat actor
Application Container Security, Operations, and Management	Container security and monitoring tools should be integrated with security information and event management (SIEM) tools to ensure container-related events are captured by the enterprise. Alternatively, in cases where the uses and privileges of containers are appropriately constrained by the orchestration layer, agencies may rely on SIEM tools present at that layer. In general, Federal agencies shall ensure that their cyber hunt and incident response teams have appropriate tools and training to identify incidents within a containerized environment.[10]
Advanced Centralized Access	Required Logs across all criticality levels shall be accessible to the highest-level security operations at the head of each agency.

[10] Reference NIST SP 800-191, Application Container Security Guide; https://csrc.nist.gov/publications/detail/sp/800-190/final

Appendix B: Definitions

The definitions for the fields in Appendix C are as follows:

Log Category – This column describes the various log categories from which logging data can be sourced. The table in Appendix C is organized by log category for ease of use.

Required Data – This column describes the information that agencies must collect within each log category.

Format – This column describes the acceptable formats for the required data. See below for definitions of the various formats that can appear in this column.

- **Attachment** – An attachment is a file sent via email.
- **Config** – A CONFIG file is a configuration file used by various applications. It contains plain-text parameters that define settings or preferences for building or running a program.
- **Database record** – A database record is a set of database fields.
- **Database query** – A database query is a request to access data from a database. Capturing the query allows for playback so that Hunt and IR teams can identify what data was exfiltrated or inserted.
- **File** – A file is a resource for recording data in a storage device.
- **Log** – A log file contains data about an event that occurred in an application or operating system.
- **Packet capture** – Packet capture (PCAP) results from the interception and copying of a data packet that is crossing or moving over a specific computer network.
- **Script** – A script file is a configuration file that lets users run or execute certain actions.
- **Simple Network Management Protocol (SNMP)** – SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB), which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

Application monitoring dashboard – An application monitoring dashboard provides information about the metrics, usage, and performance of an application. Agencies should use a dashboard suited to the version, type, and deployment method of each application.

Criticality – Each log category has an assigned criticality level based on its relative cybersecurity value. This cybersecurity value relates to the usefulness of the log data for threat detection, with the most useful data assigned a criticality of zero, and the least a criticality of 3.

Active storage – Refers to data that is stored in a manner that facilitates frequent use and ease of access.

Cold data storage – refers to the storage of data in a manner that minimizes costs while still allowing some level of access and use. Agencies should leverage architectures defined in NIST 800-92 to ensure that data stored in this manner is properly secured and audited.

EMM – Enterprise Mobility Management

UEM – Unified Endpoint Management

MTD – Mobile Threat Defense

MDM – Mobile Device Management

IMEI – International Mobile Equipment Identity

IMSI – International Mobile Subscriber Identity

Appendix C: Logging Requirements – Technical Details

Exceptions to requirements set below:

- Full packet capture data is required to be stored for only 72 hours.
- The retention periods prescribed below are minimum values; agencies may retain data for longer periods if appropriate.

Table 5: Logging Requirements – Technical Details

Log Category	Required Data	Format	Criticality	Retention Period

Identity & Credential Management	**Identity & Credential Management**
	• Account Creation
	• Manage Credential Type
	  ○ (PIV or CAC) and Derived Credentials
	  ○ Cert
	  ○ MFA
	  ○ Password
	• Establish/Manage Attributes
	  ○ Organization
	  ○ Groups/Roles
	• Manage/Track Changes in Attributes & Credentials
	• Track Usage of Credentials
	• Account Deletion
		Log
		
		Script
			0	12 Months Active Storage
				
				18 Months Cold Data Storage

Privileged Identity & Credential Management	**Privileged Identity & Credential Management**
	• Provisioning
	• Manage Credential Type
	  ○ (PIV or CAC) and Derived Credentials
	  ○ Cert
	  ○ MFA
	  ○ Password
	• Establish/Manage Attributes
	  ○ Organization
	  ○ Groups/Roles
	• Manage/Track Changes in Attributes & Credentials
	• Track Usage of Credentials
	• Deprovisioning
	• Establish and Manage Privileges (Privilege Credentials)
		Log
		
		Script
			0	12 Months Active Storage
				
				18 Months Cold Data Storage

	• Isolate, Monitor, Record, Audit Privilege Sessions
	• Control Privileged Actions
	  o Commands
	  o Tasks
	• Track Privilege Escalation and Delegation
	• Monitor, Alert and Respond to Anomalous Behaviors/Activities			

Email Filtering, Spam, and Phishing	**IP and Domain Reputation (As Indicated by Mail Server Connection)**	Log	0	12 Months Active Storage 18 Months Cold Data Storage

Network Device Infrastruc-ture (For Devices with Multiple Interfaces: Interface MAC - If Correlated to the De-NAT IP Address)	**All Devices**
	• DHCP Lease Information Including:
	  o MAC
	  o IP
		Log	0	12 Months Active Storage
				
				18 Months Cold Data Storage

Network Device Infrastruc-ture	**DNS - Source IP and Port, Destination IP and Port** **Date and Time** • Content of Query, Response, and Errors – All Record Types • Zone Transfers Request and Response (Audit Log) • Zone Transfers Request and Response (Content)	Log	0	12 Months Active Storage 18 Months Cold Data Storage

Network Device Infrastruc-ture	**Passive DNS Log** • Tuple (Rrname, Rrtype, Rdata) • Time_First • Time_Last • Count • Bailiwick • Sensor_Id • Zone_Time_First • Zone_Time_Last • Time_First_Ms • Time_Last_Ms • Origin • Count of Questions Asked by Source IP • Count of Questions Asked Overall • Count of Responses by Source IP • Query Size in Bytes • Response Size in Bytes • TTL per Record Returned • Request Was Made Via UDP, TCP or Both • Response Was Made Via UDP, TCP or Both • Passive DNS Source (Used to Identify Which Passive DNS Source Data Came From)	Log Database Record	0	12 Months Active Storage 18 Months Cold Data Storage
Network Device Infrastruc-ture	**DNS, DHCP, and Wi-Fi** • Wi-Fi Supporting Infrastructure Logs Including Security Logs at Info Level • Device Authentication Logs with User Agent • URL Browsing Logs + HTTP Methods (e.g., Post, Get, etc.) • User Authentication Logs • DHCP Lease Information Including MAC, IP • Roaming Logs • Timestamps	Log SNMP	0	12 Months Active Storage 18 Months Cold Data Storage

Network Device Infrastructure	**DNS, DHCP, and Wi-Fi**
	• Static Network Address Translation Table Mapping as Well as Port Forwards
	  ○ Date and Time
	  ○ Protocol
	  ○ Port
	  ○ Inside Local and Global IP and Port
	  ○ Outside Local and Global IP and Port
		Log
		
		Database Record
		
		Script
		
		File
		
		Config
		
		SNMP
			0	12 Months Active Storage
				
				18 Months Cold Data Storage

Network Device Infrastructure (General Logging)	• IDS / IPS / NTA / NDR / SIEM Logs • API Activity Logs • Authentication Logs • Firewall Logs • Web Proxy/WAF Logs • Service Metrics • Network Flow Logs • Remote Access/VPN Logs • System/OS Logs • DLP Logs • DNS Query/Response Logs	Log File Packet Capture	0	12 Months Active Storage 18 Months Cold Data Storage 72 Hours Packet Capture
Network Device Infrastructure (For Devices with Multiple Interfaces: Interface MAC - If Correlated to The De-NAT IP Address)	**Routers and Switches** • Routing Tables • Routing Changes (Logging All CLI Commands, BGP) • IP Addressing Schema and Implementation	Script File Config	0	12 Months Active Storage 18 Months Cold Data Storage

Network Device Infrastruc-ture (For Devices with Multiple Interfaces: Interface MAC - If Correlated to the De-NAT IP Address)	**Load Balancer / Reverse Proxy** Access Logs • Connection Type • Date and Time • Resource ID of the Load Balancer • Client IP:Port • Target IP:Port • Request Processing Time • Target Processing Time • Response Processing Time • Status Code from Load Balancer • Target Status Code • Received Bytes • Bytes Sent • Request • User Agent • SSL Cipher • SSL Protocol • SNI Domain • Matched Rule Priority • Actions Executed • Redirect URL • Error Reason • Target IP:Port List • Target Status Code List • Classification Reason Request Does Not Comply with RFC 7230 • Other Implementation Specific Fields	Log	0	12 Months Active Storage 18 Months Cold Data Storage

Network Device Infrastructure (For Devices with Multiple Interfaces: Interface MAC – If Correlated to the De-NAT IP Address)	**Proxies and Web Content Filters**
	Provides NAT, User, and Gateway IP Address to Provide Enhanced Reporting of Malicious Domains and IP Addresses. In the Case of Web, W3c Format.
	• Date and Time
	• Source
	  ○ Hostname
	  ○ IP Address and Port
	  ○ MAC
	• Destination
	  ○ Hostname
	  ○ IP Address and Port
	  ○ MAC
	• Web URL Methods / User Agent / Decoded Headers
	• URL Categories
	• URL
	• Permitted, Restricted, Denied
		Log	0	12 Months Active Storage
				
				18 Months Cold Data Storage

Network Device Infrastructure	**Proxies and Web Content Filters** • Policy Updates • Software Updates	Log	0	12 Months Active Storage 18 Months Cold Data Storage
Network Device Infrastructure (Access, Authorization, and Accounting)	**General Information** • Date and Time • Event, Status, or Error Codes • Service/Command/Application Name • User or System Account Associated with an Event • Device Used (e.g., Source and Destination IPs, Terminal Session ID, Web Browser, etc.) **Operating System (OS) Events** • Start-Up and Shutdown of the System • Start-Up and Shutdown of a Service	Log	0	12 Months Active Storage 18 Months Cold Data Storage

	• Network Connection Changes or Failures
	• Changes to, or Attempts to Change, System Security Settings and Controls
	
	OS Audit Records
	• Log-On Attempts (Success/Failure)
	• The Function(s) Performed after Logging On (e.g., Reading or Updating a Critical File, Software Installation)
	• Account Changes (e.g., Account Creation and Deletion, Account Privilege Assignment)
	• Successful/Failed Use of Privileged Accounts
	
	Application Account Information
	• Application Authentication Attempts (Success/Failure)
	• Application Account Changes (e.g., Account Creation and Deletion, Account Privilege Assignment)
	• Use of Application Privileges
	
	Application Operations
	• Application Startup and Shutdown
	• Application Failures
	• Major Application Configuration Changes
	• Application Transactions, For Example,
	  ○ Email Servers Recording the Sender, Recipients, Subject Name, and Attachment Names for Each Email
	  ○ Web Servers Recording Each URL Requested and the Type of Response Provided by the Server			

	○ Business Applications Recording Which Financial Records Were Accessed by Each User			
Operating Systems - Windows Infrastruc-ture and Operating Systems	**User and Administrator Access to OS Components and Applications** • File and Object Access • Audit Log Access (Success/Failure) • System Access and Log Off (Success/Failure) • Privilege Access and Log Off (Success/Failure) • RDP Access and Log Off (Success/Failure) • SMB Access • Installation or Removal of Storage Volumes or Removeable Media **System Performance and Operational Characteristics** • Resource Utilization, Process Status • System Events • Service Status Changes (Start, Stop, Fail, Restart, etc.) • Service Failures and Restarts • Process Creation and Termination **System Configuration** • Changes to Security Configuration (Success/Failure) • Audit Log Cleared • Changes to Accounts • User or Group Management Changes • Scheduled Task Changes **File Access** • Transfer of Data to External Media or Remote Hosts	Log	0	12 Months Active Storage 18 Months Cold Data Storage

	Host Network Communications • Listening Network Port and IP Address • Active Network Communication with Other Hosts **Powershell Execution Commands** **WMI Events** **Registry Access** **Command-Line Interface (CLI)** **Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware** • Version • Created Date • Installed Date • Manufacturer			

Operating Systems - MACOS (Or Other Apple Desktop and Server Operating Systems)	**User and Administrator Access to OS Components and Applications** • File and Object Access • Audit Log Access (Success/Failure) • System Access and Log Off (Success/Failure) • Privilege Access and Log Off (Success/Failure) • Remote Terminal or Equivalent Access and Log Off (Success/Failure) • Samba/NFS/(S)FTP or Equivalent Access • Installation or Removal of Applications • Installation or Removal of Storage Volumes or Removeable Media **System Performance and Operational Characteristics** • Resource Utilization, Process Status • System Events • Service Status Changes (Start, Stop, Fail, Restart, etc.) • Service Failures and Restarts • Process Creation and Termination **System Configuration** • Changes to Security Configuration (Success/Failure) • Audit Log Cleared • Changes to Accounts • User or Group Management Changes • Scheduled Task Changes **File Access** • Transfer of Data to External Media or Remote Hosts **Host Network Communications**	Log	0	12 Months Active Storage 18 Months Cold Data Storage

	• Listening Network Port and IP Address • Active Network Communication with Other Hosts **Command-Line Interface (CLI)** • System Log Folder: /Var/Log/* • System Log: /Var/Log/System.Log • Mac Analytics Data: /Var/Log/Diagnosticmessages/* • Wi-Fi Log: /Var/Log/Wifi.Log • System Application Logs: /Library/Logs/* and /Private/Var/Log/* • System Reports: /Library/Logs/Diagnosticreports/* • User Application Logs: /Users/Name/Library/Logs/* • User Reports: /Users/Name/Library/Logs/Diagnosticreports/* • Audit Log: /Var/Audit/* **Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware** • Version • Created Date • Installed Date • Manufacturer			

Operating Systems – BSD (Linux)	**User and Administrator Access to OS Components and Applications** • File and Object Access • Audit Log Access (Success/Failure) • System Access and Log Off (Success/Failure) • Privilege Access and Log Off (Success/Failure) • Remote Terminal or Equivalent Access and Log Off (Success/Failure) • Samba/NFS/(S)FTP or Equivalent Access • Installation or Removal of Storage Volumes or Removeable Media **System Performance and Operational Characteristics** • Resource Utilization, Process Status • System Events • Service Status Changes (Start, Stop, Fail, Restart, Etc.) • Service Failures and Restarts • Process Creation and Termination **System Configuration** • Changes to Security Configuration (Success/Failure) • Audit Log Cleared • Changes to Accounts • User or Group Management Changes • Scheduled Task Changes **File Access** • Transfer of Data to External Media or Remote Hosts **Host Network Communications** • Listening Network Port and IP Address	Log	0	12 Months Active Storage 18 Months Cold Data Storage

	• Active Network Communication with Other Hosts **Command-Line Interface (CLI)** **Security Enhanced Linux (SELinux) AppArmor or Equivalent** • Warning Logs • Violation Logs **System** • /Var/Log/Messages • /Var/Log/Dmesg • /Var/Log/Syslog • /Var/Log/Daemon.Log • /Var/Log/Cron • /Var/Log/Kern.Log • /Var/Log/Boot.Log **Access And Authentication** • /Var/Log/Auth.Log • /Var/Log/Secure • /Var/Log/Faillog • /Var/Log/Btmp • /Var/Log/Wtmp or /Var/Log/Utmp **Applications** • /Var/Log/Mail.Log or /Var/Log/Maillog • /Var/Log/Xorg.X.Log **Package Install/Uninstall** • /Var/Log/Dpkg.Log • /Var/Log/Yum.Log **Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware** • Version • Created Date • Installed Date • Manufacturer			

Cloud Environments (General Events)	Nearly all successful attacks on cloud services result from customer misconfigurations. With that in mind, the logging and monitoring focus should be on: • Any Activity on Breakglass Account(s) (which should never have to be used) • Conditional Access Policy Changes • Changes to Environment Policies (e.g., Azure Subscription, AWS Services, Google Solutions, etc.) in Management Logs • Privileged Role Changes • Virtual Network (VNet) Changes • Deletions of Delete Locks • Changes to Logging Policies • Privileged Identity Management (PIM) and Identity Protection Changes • Changes to Alert Rules (Audit the Auditor) • Key Vault/Key Management Changes • Storage File Access Logs, File, File Hashes • Baseline Deviations for Prod App Tiers • Baseline Deviations for Prod Data Tiers	Log	0	12 Months Active Storage 18 Months Cold Data Storage

Cloud Environ-ments (General Logging)	• IDS / IPS / NTA / NDR / SIEM Logs • API Activity Logs • Authentication Logs • Firewall Logs • Web Proxy/WAF Logs • Service Metrics • Billing Data • Flow Logs • Remote Access/VPN Logs • System/OS Logs • DLP Logs • DNS Query/Response Logs	Log	0	12 Months Active Storage 18 Months Cold Data Storage 72 Hours Packet Capture
Cloud AWS	• AWS Cloudtrail • Amazon Cloudwatch Logs • AWS Config • Amazon S3 Access Logs • Amazon VPC Flow Logs • AWS WAF Logs • AWS Shield • AWS Guardduty • AWS Security Hub	Log	0	12 Months Active Storage 18 Months Cold Data Storage
Cloud Azure	• Azure Active Directory Logs • Activity Logs • Unified Audit Logs (w/ Advanced Audit Features)	Log	0	12 Months Active Storage 18 Months Cold Data Storage
Cloud GCP	• Access Transparency Audit Log • Admin Audit Log • Data Studio Audit Log • Drive Audit Log • Email Audit Log • Groups Audit Log • LDAP Audit Log • Login Audit Log • Devices Audit Log • Sail Audit Log • Token Audit Log • User Accounts Audit Log • OAuth Token Audit Log • Security Reports	Log	0	6 Months Active Storage 18 Months Cold Data Storage

	• Usage Logs • Storage Logs • Data Access Logs For Organizational and Default Configuration Settings Enable: • Admin Read • Data Read • Data Write			
System Configura-tion and Performanc e	**Configuration** – Scripts or Database Changes Used to Configure Systems, Services on a System, or Applications	Database Record Script	1	12 Months Active Storage 18 Months Cold Data Storage
System Configura-tion and Performanc e	**Endpoint Detection & Response (EDR)**	Log	1	12 Months Active Storage 18 Months Cold Data Storage
System Configura-tion and Performanc e	**Configuration Changes** • Management Action (Success/Failure) • Admin Login (Success/Failure)	Log	1	12 Months Active Storage 18 Months Cold Data Storage

Authentication and Authorization[11]	**Administrative**
	• Authentication Logons (Success/Failure)
	• Authentication Logoffs
	• Privilege Elevation (Success/Failure)
	• Security Related System Alerts and Failures
	• User and Group
	  ○ Additions
	  ○ Deletions
	  ○ Modification to Permissions
	• Unauthorized Access Attempts to Critical Systems and File
		Log	1	12 Months Active Storage
				
				18 Months Cold Data Storage

Authentication and Authorization[12]	**Authorization** All Privileged Operations Including: • "sudo" or runas • Enabling CLI Access • System Administrative Commands • Powershell Execution Commands • Powershell Script Block Logging	Log	1	12 Months Active Storage 18 Months Cold Data Storage
Email Filtering, Spam, and Phishing	**Content Filtering Policy Updates**	Log	1	12 Months Active Storage 18 Months Cold Data Storage

Anti-Virus and Behavior-Based Malware Protection	• Date and Time
	Source Hostname
	  ○ IP
	  ○ Port
	• Destination Hostname
	  ○ IP
	  ○ Port
	• Description of Malicious Code or Action and Severity
		Log
		
		Email Attachments
			1	12 Months Active Storage
				
				18 Months Cold Data Storage

[11] These requirements are general requirements that apply to systems and applications that are not specified in this document

[12] These requirements are general requirements that apply to systems and applications that are not specified in this document

	• Identity or (Hash) Identifier of the File(s) • Description of the Action Taken (Clean, Quarantine, Delete) • Signature Updates			
Anti-Virus and Behavior-Based Malware Protection	**Indication of the Host that Connected to a Specific URL** • Date and Time • IP and Domain Reputation • URL • Categorization	Log	1	12 Months Active Storage 18 Months Cold Data Storage

Network Device Infrastruc-ture	**All Devices**
	• Hash of the Binary / Binaries Running on the Device
	• Hash of Configs
	• Firmware
	  ○ Version
	  ○ Created Date
	  ○ Installed Date
	  ○ Manufacturer
		Script
		
		File
			1	12 Months Active Storage
				
				18 Months Cold Data Storage

Network Device Infrastruc-ture (for Devices with Multiple Interfaces: Interface MAC - If Correlated to the De-NAT IP Address)	**Firewalls**
	All Events from Firewall. At the very least, if access control lists (ACL) are enabled and the device is filtering traffic:
	• Action Permit, Teardowns, Closes, Denies, and Drops
	• Interface
	• Source
	  ○ Hostname
	  ○ IP Address and Port
	  ○ MAC
	• Destination
	  ○ Hostname
	  ○ IP Address and Port
	  ○ MAC
	• Protocol Type
	• Rule Name and Number Triggered
	• URL if Applicable, Associated User and User Agent
	• Date and Time
		Log	1	12 Months Active Storage
				
				18 Months Cold Data Storage

Network Device Infrastruc-ture (For Devices with Multiple Interfaces: Interface MAC - if Correlated to the De-NAT IP Address)	**All Devices: IDs / IPs Alerts and Events**
	• Date and Time
	• Source
	  ○ Hostname
	  ○ IP Address and Port
	  ○ MAC
	• Destination
	  ○ Hostname
	  ○ IP Address and Port
	  ○ MAC
	• Signature Triggered and Associated Details Including:
	  ○ Signature
	  ○ Anomaly
	• Rate Threshold
	• Device Name
	• Type of Event and Category
	• In the Case of Fortinet Network IPs, Attack Context
	• (Web / Device) User Agent if Available
	• Wi-Fi Channel
	• Wi-Fi Extended Service Set Identifier (ESSID)
		Log	1	12 Months Active Storage
				
				18 Months Cold Data Storage

Network Device Infrastruc-ture (For Devices with Multiple Interfaces: Interface MAC - if Correlated to the De-NAT IP Address)	**VPN Gateway – All Events**
	At the very least, for Accepts, Teardowns, Closes, Denies, and Drops:
	• Date and Time
	• Source
	  ○ Hostname
	  ○ IP Address and Port
	  ○ MAC
	• Destination
	  ○ Hostname
	  ○ IP Address and Port
	  ○ MAC
	• Source IP Address and Port, MAC (Inside Tunnel)
	• Destination IP Address and Port, MAC (Inside Tunnel)
	• Authentication Information (Success/Fail with Username and Device with User Agent)
		Log	1	12 Months Active Storage
				
				18 Months Cold Data Storage

	• Change in Status of Connections / Tunnel Status • VPN Certificate Status Validation			
PKI Infrastruc-ture	All Events Related to: • Generation • Revocation • Access • Update • Expiry • Recover • Authentication Success • Authentication Fail • LDAP Logs	Log	1	12 Months Active Storage 18 Months Cold Data Storage
Vulnerabil-ity Assessment s	• Date and Time • Hostname, IP Address, and OS Version • Open Ports • Installed Applications • Version of Installed Applications • Vulnerabilities Listed in Installed Applications • Source of Vulnerability and Severity	Log[13]	1	12 Months Active Storage 18 Months Cold Data Storage

[13] Logs are kept for ALL assessments, even if there are 0 vulnerabilities identified during the assessment

Database Level	• Addition of New Users, Especially Privileged Users
	• Query Being Executed
	• Query, Status (Response), and Traceback
	  ○ Method
	  ○ Comments or Variables
	  ○ Multiple Embedded Queries
	  ○ Database Alerts or Failures
	  ○ Time to Execute Query
	• Attempts to Elevate Privileges (Success/Failure)
	• Changes to the Database Structure
	• Changes to User Roles or Database Permissions
	• Database Administrator Actions
	• Database Logons (Success/Failure)
	• Failed Logons
	• Use of Executable Commands
	• CLI Commands against the Data Base
	• Database Configuration and Version
	• Access to Sensitive Information within the Databases such as Keys, Passwords, Privacy Related Data
		Log
		
		Database Query
			1	12 Months Active Storage
				
				18 Months Cold Data Storage

Application Level	**Web Applications** • URL • Headers • HTTP Methods - Request with Body of Data[14] • HTTP Response with Body of Data	Log Log and PCAP of Plaintext HTTP Request and	1	12 Months Active Storage 18 Months Cold Data Storage

[14] Agencies shall evaluate this data to ensure proper protections are in place to encrypt the data at rest and in transit. Agencies shall also ensure that their tools are accredited to handle sensitive data and proper oversight controls are implemented to look for signs of inappropriate data usage

		Response with Data		72 Hours Packet Capture
Application Level	**Web Application** • Database Queries • Response Codes	Log	1	12 Months Active Storage 18 Months Cold Data Storage
Application Level	**Web Application Crashes** • Processes • Applications	Log	1	12 Months Active Storage 18 Months Cold Data Storage
Application Level	**Web Applications & Middleware** • Configuration • Version	Log	1	12 Months Active Storage 18 Months Cold Data Storage

Virtualization System	• User Authentication
	  ○ Logon (Success and Failure)
	  ○ Attempts to Obtain Privileged Access (Success and Failure)
	• User and Administrator/Root Access and Actions of Components and Applications
	  ○ File and Object Access
	  ○ Audit Log Access (Success and Failure)
	  ○ System Access (Failure)
	• System Performance and Operational Characteristics
	  ○ Resource Utilization, Process Status
	  ○ System Events
	  ○ Service Status Changes (e.g., Started, Stopped)
	• System Configuration
	  ○ Changes to Security Configuration (Success/Failure)
	  ○ Changes to Hypervisor
	  ○ Changes to VMS
	  ○ Changes Made within VMS
	  ○ Audit Log Cleared
	• Creation and Deployment of VMS
	• Migration of VMS (e.g., Source and Target Systems, Time, Authorization)
	• Creation and Deletion of System-Level Objects
		Log	1	12 Months Active Storage
				
				18 Months Cold Data Storage

Mobile (Smart-phones and Tablets) EMM (UEM) / MTD Server Logs	**EMM (UEM)/MTD Alerts** • Date and Time • Alert Type • Failure of Cryptographic Protocols • Failure of Device Cryptographic Capabilities (e.g., Trusted Boot Process)	Log	1	12 Months Active Storage 18 Months Cold Data Storage

	• Certificate Validation Failure (Defined in MDM Server Protection Profile) • Alerts from Agent to Server Defined MDM Agent Protection Profile			
Mobile (Smart-phones and Tablets) EMM (UEM) / MTD Agent Logs	**General:** • Date and Time **Device Data** • Device Name • Device Manufacturer and Model • Serial # • Phone # • IMEI, IMSI, OS Version, OS Build • Firmware Version • Device IP Address, Device Root/Jailbreak Status and Reasons • Developer Mode Enabled • Battery/Power Information • Hardware Info (Processor, Memory, Storage) • Last Time Device Synched with Enterprise **Application Data** • Application Manifest (Installed Apps, App Version, Version History and Installation Timestamps), Installation and Data Storage Location • Application Permissions • Application Hash (e.g., SHA-256) • Running Apps and Processes **Device Policy Settings** • Enrollment Policies • Policies Successfully/Unsuccessfully Applied	Log	1	12 Months Active Storage 18 Months Cold Data Storage

	• Authentication Policies (Password/Pin/Biometric, etc.) **Device Configuration** • Certificates end Related Information (Validity Period, Revocation, etc.) • Device Encryption Configuration • Android Enterprise Settings • System Integrity Status **Network Configuration** • Allowed/Disallowed Networks • Currently Connected Network • Proxy/Tunnel and Per-App VPN Info • Telephony Info (Some of This Is Covered by Carrier Data) • Captive Portals • Wi-Fi SSID • Network MAC Address • Bluetooth **Event / Audit / Crash Logs** • Event Type and ID • Event Date/Timestamp • Success/Failure of Various Services • User Authentication (Success/Failure) • Event Actor and ID (e.g., Admin, System, Device) • Event Change Type (CRUD) **MTD Agent Info** • Agent Activation Status • Threat Detection of Variety of Vulns • Phishing Protection Status • Tampering of Agent, App, or System • Privilege Escalation • MITM Activities • Remediation Actions Taken			

	• Last Time Device Synched with Enterprise			
Container - Supply Chain	• Log Container Image Sources • Log Changes / Deltas Between Image Source Versions • Log Vulnerability Scan of Container Images, even if No Vulnerabilities Are Discovered • Log Where Containers Are Deployed and Which System They Support	Script Manual Log Entry	1	12 Months Active Storage 18 Months Cold Data Storage
System Configura-tion and Performanc e	**System Status** • Resource Utilization • Performance	Log Database Record Script	2	12 Months Active Storage 18 Months

				Cold Data Storage

Email Filtering, Spam, and Phishing	**Raw and Metadata - Filtering Events**[15]
	• Date and Time
	• Sent from Sender, from Sender
	• Recipient
	• Subject
	• Email Headers
	• Rule Triggered – Log of Policies along with Actual Values Including but Not Limited to:
	  ○ DNS Records
	  ○ Phish Campaign Identifier
	  ○ Domain URL
		Log
		
		Email Attach-ments
			2	12 Months Active Storage
				
				18 Months Cold Data Storage

Data Loss Prevention	• Date and Time
	• Source Hostname
	  ○ IP
	  ○ Port
	• Destination Hostname
	  ○ IP
	  ○ Port
	• Description of Malicious Code or Action and Severity
	• Identity or Identifier of the File(s)
	• Description of the Action Taken (Clean, Quarantine, Delete)
	• Signature Updates
		Log
		
		Email Attach-ments
			2	12 Months Active Storage
				
				18 Months Cold Data Storage

Network Traffic	**Full Packet Capture Data** • Decrypted Plaintext • Cleartext	Packet Capture	2	72 Hours Packet Capture

[15] Federal agencies shall submit all phishing attempts to CISA by forwarding the phishing as an attachment to federal.phishing.report@us-cert.gov. Federal agencies shall ensure that all contractors that operate infrastructure on their behalf implement this requirement.

Application Level	• **Commercial Off the Shelf (COTS) and Custom Applications**
	• User Authentication (Success/Failure)
	• User and Administrator Application Use:
	  o File and Object Access
	  o Audit Log Access (Success/Failure)
	  o System Access (Failure)
	  o Application Transactions (Web Page Hits, Email Sent/Received, File Transfers Completed)
	• Transaction Logs
	• System Performance and Operational Characteristics
	  o Resource Utilization
	  o Process Status
	  o Errors (Input Validation, Dis-Allowed Operations)
	  o System Events
	  o Service Status Changes (e.g., Started, Stopped)
	• Application Configuration and Version
		Log
		
		Application Monitoring Dashboards
			2	12 Months Active Storage
				
				18 Months Cold Data Storage

Application Level	**General – Non-COTS**
	• User Authentication (Success/Failure)
	• User Access of Application Components
	  o File and Object Access
	  o Audit Log Access (Success/Failure)
	  o System Access (Failure)
	  o Application Transactions
	• Transaction Logs
	• System Performance and Operational Characteristics
	  o Resource Utilization
	  o Errors (Input Validation, Dis-
		Log	2	12 Months Active Storage
				
				18 Months Cold Data Storage

	Allowed Operations) and Exit Codes ○ Process Status ○ Service Status Changes (e.g., Started, Stopped) • Application Configuration and Version, Middleware Configuration and Version • Usage Information, if Applicable • User Request and Response Events, if Applicable			
Container - Image	• Vulnerability Scan Log • Hash of the Binary • Hash of the Executables • Container-Aware Network Monitoring • Container-Aware Process Monitoring • Container-Aware Malware Detection • Filesystem Changes Log • Data Monitoring • Read and/or Writes to Well-Known Directories (e.g., /ETC, /USR/BIN, USR/SBIN, etc.) • Creating Symlink • Changes in File/Resource Ownership or Mode Changes (CHMOD) • Access Control Log • Runtime Vulnerability Scan Log Scan for Malware Log • Digital Signature Verification • Unexpected Network Connections or Socket Mutations • Spawned Processes Using Things Like <Execve> • Executing Shell and/or SSH Binaries	Log File Script	2	12 Months Active Storage 18 Months Cold Data Storage

Container - Engine (Management / Orchestration)	• Audit Log • Account Access Log • Account Permission Changes • Configuration Log • Resource Allocation and Consumption • Registration Changes	Log Application Monitoring Dashboards	2	12 Months Active Storage 18 Months Cold Data Storage

Container - OS	• User and Administrator Access to OS Components and Applications
	  ○ File and Object Access
	  ○ Audit Log Access (Success/Failure)
	  ○ System Access and Log Off (Success/Failure)
	  ○ Privilege Access and Log Off (Success/Failure)
	  ○ RDP Access and Log Off (Success/Failure)
	  ○ SMB Access
	• System Performance and Operational Characteristics
	  ○ Resource Utilization, Process Status
	  ○ System Events
	  ○ Service Status Changes (Start, Stop, Fail, Restart, etc.)
	  ○ Service Failures and Restarts
	  ○ Process Creation and Termination
	• System Configuration
	  ○ Changes to Security Configuration (Success/Failure)
	  ○ Audit Log Cleared
	  ○ Changes to Accounts User or Group Management Changes
	  ○ Scheduled Task Changes
	• File Access
		Log	2	12 Months Active Storage
				
				18 Months Cold Data Storage

	○ Transfer of Data to External Media • Powershell Execution Commands • WMI Events • Registry Access • Command-Line Interface (CLI)			
System Configuration and Performance	**Software Updates** • User Agent	Log Database Record Script	3	12 Months Active Storage 18 Months Cold Data Storage
Email Filtering, Spam, and Phishing	**Spam Dictionary Modifications**	Log	3	12 Months Active Storage 18 Months Cold Data Storage
Mainframes	• Syslog & Syslogd Data • Log4j Data • Sysout Data Resource Measurement Facility (RMF) Data • System Management Facility (SMF)[16] • Output from Integrated Intrusion Detection Services	Log	3	12 Months Active Storage 18 Months Cold Data Storage

[16] DOD Security and Technical Implementation Guide (STIG) for zOS for log configuration guidance, https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_IBM_zOS_Y21M07_STIG.zip

Container - Cluster/Pod Events	• Container User and Service Logs • Container and Application API Audit Logs • Container Management Access Logs • Changes to Container Resources Across Containers and Container Management Environment	Log	3	Container - Cluster/Pod Events