EFFECTIVE DATE

(07-27-2023)

PURPOSE

(1) The purpose of the new Internal Revenue Manual (IRM) 10.8.63, **Information Technology (IT) Security, Central Log Server Security Policy** is to provide guidance and establish security requirements necessary to implement and manage IT security for centralized log servers within the IRS.

MATERIAL CHANGES

(1) The Oversight & Strategic Management Security Policy office is introducing new IT Policy for Central Log Server Security.

EFFECT ON OTHER DOCUMENTS

This IRM supplements IRM 10.8.1, *Information Technology (IT) Security Policy and Guidance*; IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*.

AUDIENCE

IRM 10.8.63 shall be distributed to all personnel responsible for overseeing, managing, and implementing centralized log server security for IRS information systems. The Centralized Log Server Security Policy will consist of, but not limited to, agency–defined requirements, authoritative guidance, legislative mandates, and national standards. This policy applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya
Acting, Chief Information Officer

10.8.63
Central Log Server Security Policy

Table of Contents

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

Exhibits

#

10.8.63.1
(07-24-2023)
Program Scope and Objectives (SPDER)

(1) **Overview**: This Internal Revenue Manual (IRM) lays the foundation to implement and manage security controls and guidance for the use of centralized log servers within the Internal Revenue Service (IRS).

   a. This manual is subordinate to IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* and augments the existing requirements identified within IRM 10.8.1, as they relate to IRS centralized logging server security.

(2) **Purpose of the Program**: Develop and publish security policies to protect the IRS against potential IT threats and vulnerabilities and ensure compliance with federal mandates and legislation.

(3) **Audience**: The provisions within this manual apply to:

   a. All offices and business, operating, and functional units within the IRS.
   b. Individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors and outsourcing providers, which use or operate systems that store, process, or transmit IRS information or connect to an IRS network or system.

(4) **Policy Owner**: Chief Information Officer

(5) **Program Owner**: Cybersecurity, Threat Response and Remediation (an organization within Cybersecurity)

(6) **Program Goals**: To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.63.1.1
(07-24-2023)
Background

(1) The centralization of event logging allows security personnel to rapidly visualize data from many sources to spot trends and complex attacks on enterprise assets. This IRM supports this goal by providing the technical security policies and requirements for applying security concepts to Security Information and Event Management servers (SIEMs), syslog servers, Network Management Systems (NMSs), and other event-based aggregation and monitoring applications that are part of the events logging, notification, monitoring, and analysis functions in the enterprise.

   a. The scope of this IRM includes applications that leverage aggregated audit logs collected from firewalls, routers, servers, applications, and databases to visualize, monitor, notify, and alert based on identified thresholds.
   b. Throughout this IRM, log, audit, and events records are used interchangeably and are understood to have similar meaning. Auditable events are those activities that can be tracked that provide information regarding system resource usage. These events are captured as part of the configuration of the operating systems or network management function of the hosts and devices on the network. In a typical hierarchy, all auditable records are sent to a syslog server that is configured on the host or device. The syslog daemon receives logs directed at it and aggregates the records.

(2) IRM 10.8.63 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.63.1.2
(07-24-2023)
Authority

(1) All IRS systems and applications shall be compliant with Executive Orders (EOs), Office of Management and Budget (OMB), Federal Information Security Modernization Act of 2014 (FISMA), National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), National Archives and Records Administration (NARA), The Department of the Treasury, and IRS guidelines as they apply.

10.8.63.1.3
(07-24-2023)
Roles and Responsibilities

(1) IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*, defines IRS-wide roles and responsibilities related to IRS information and information system security, and is the authoritative source for such information.

10.8.63.1.4
(07-24-2023)
Program Management and Review

(1) The IRS Cybersecurity Program establishes a framework of security controls to ensure the inclusion of security in the daily operations and management of IRS IT resources. This framework of security controls is provided through the issuance of security policies via the IRM 10.8.x series and the development of technology specific security requirement checklists. Stakeholders are notified when revisions to the security policies and security requirement checklists are made.

10.8.63.1.5
(07-24-2023)
Program Controls

(1) Each IRM in the 10.8.x series is assigned an author who reviews their IRM annually to ensure accuracy. The IRM authors continuously monitor federal guidance (e.g., OMB, CISA, NIST, Defense Information Systems Agency (DISA)) for potential revisions to security policies and security requirement checklists. Revisions to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.

(2) Security Policy provides a report identifying security policies and security requirement checklists that have recently been revised or are in the process of being revised.

(3) This IRM applies to all IRS information and information systems, which include IRS production, development, test, and contractor systems. For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *Classified National Security Information (NSI)*, for additional guidance for protecting classified information.

(4) This IRM establishes the minimum baseline security policy and requirements for all IRS centralized log servers in order to:

a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.
b. Prevent unauthorized access to IRS assets.
c. Enable IRS IT computing environments to meet the security requirements of this policy and support the business needs of the organization.

(5) In the event there is a discrepancy between this policy and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls/requirements in this policy are more restrictive.

10.8.63.1.6
(07-24-2023)
Terms and Acronyms

(1) Refer to Exhibit 10.8.10-2 for a list of terms, acronyms, and definitions.

10.8.63.1.7
(07-24-2023)
Related Resources

(1) Refer to Exhibit 10.8.10-3 for a list of related resources and references.

10.8.63.2
(07-24-2023)
Risk Acceptance and Risk-Based Decisions

(1) Any exception to this policy requires the Authorizing Official (AO) to make a Risk-Based Decision (RBD).

(2) Users shall submit RBD requests in accordance with Cybersecurity's Security Risk Management (SRM) Risk Acceptance Process within the Risk Based Decision Standard Operating Procedures (SOP).

#
#
#

(3) Refer to IRM 10.8.1 for additional guidance about Risk Acceptance and Risk-Based Decisions.

10.8.63.3
(07-24-2023)
IT Security Controls

(1) The security controls in this IRM supplement the requirements found in IRM 10.8.1.

a. Refer to IRM 10.8.1 for security control families and security controls not addressed within this IRM.

(2) It is acceptable to configure settings to be more restrictive than those defined in this IRM.

(3) To configure less restrictive requirements requires a risk-based decision. Refer to the Risk Acceptance and Risk-Based Decisions section within this IRM for additional guidance.

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

#
#

#
#

#
#
#

#
#
#

#

#
#
#
#
#
#
#

#

#
#
#
#
#
#
#
#
#

#
#
#

#
#

#
#
#
#
#
#

#

#
#
#
#
#

#
#

#
#

#
#

#
#

#
#
#
#

#
#

#
#
#
#

#

#
#
#
#

#

#
#
#

#
#
#
#
#

#
#
#

Any line marked with a #
is for **Official Use Only**

#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#
#

#
#
#

#
#
#

#

#
#
#
#

#
#
#
#

#
#
#
#
#
#
#
#

Any line marked with a #
is for **Official Use Only**

#
#

#
#
#

#
#

#
#
#

#
#

#
#
#

#
#

#
#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#
#

#
#
#
#
#

#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

Exhibit 10.8.63-2 (07-24-2023)
Terms and Acronyms

Term	Definition or Description
Audit	Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.
Application	An application is a software program hosted by an information system that is designed to perform a specific function directly for users / applications and can be executed without access to system control, monitoring, or administrative privileges.
AO	Authorizing Official
Authenticator	Authenticator is something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous editions of SP 800-63, this was referred to as a token. (NIST SP 800-63-3)
Contractor	Contractors are individuals or other legal entities that are, directly or indirectly, awarded government contracts. Contractors conduct business, or reasonably may be expected to conduct business, with the Government as an agent or representative of another contractor.
CIS	Center for Internet Security
CSIRC	Computer Security Incident Response Center
Cybersecurity	Cybersecurity is the ability to protect or defend the use of cyberspace from cyber attacks.
DISA	Defense Information Systems Agency
EA	Enterprise Architecture
EL	Event Logging
EMM	Enterprise Mobility Management
EO	Executive Order
ESP	Enterprise Standards Profile
FIPS	Federal Information Processing Standards (FIPS) are publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors.
FIPS-validated cryptography	A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-3 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See *NSA-approved cryptography*.

Exhibit 10.8.63-2 (Cont. 1) (07-24-2023)
Terms and Acronyms

FISMA	The Federal Information Security Modernization [FISMA] of 2014 requires federal agencies to identify and provide information security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency; or information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.
HMAC	Hash Message Authentication Code a message authentication code that uses a cryptographic key in conjunction with a hash function. (CNSSI 4009)
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IRM	Internal Revenue Manual
ISSO	Information System Security Officer
KDF	Key Derivation Functions
Log	A record of the events occurring within an organization's systems and networks.
MDM	Mobile Device Management
MFA	Multi-Factor Authentication is authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). See authenticator. (NIST SP 800-171 Rev2)
MTD	Mobile Threat Defense
NIST	National Institute of Standards and Technology
NMS	Network Management System - An application or set of applications that lets network administrators manage a network's independent components inside a bigger network management framework.
NTP	Network Time Protocol is used in networks of all types and sizes for time synchronization of servers, workstations, and other networked equipment. (CNSSI 4009)
OMB	Office of Management and Budget
Outsourcing Provider	An Outsourcing Provider is a provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. (NIST SP 800-161 from NIST SP 800-53 Rev. 4)
PCAP	Packet Capture

Exhibit 10.8.63-2 (Cont. 2) (07-24-2023)
Terms and Acronyms

PIV	Personal Identity Verification is a physical artifact (e.g., identity card, ″smart″ card) issued to a government individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). Synonymous with personal identity verification (PIV) card. Note: PIV requirements are defined in FIPS 201-2. (CNSSI 4009)
PKI	Public Key Infrastructure is a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. Class 3 PKI certificates are used for servers and software signing rather than for identifying individuals. Class 4 certificates are used for business-to-business transactions.
RBD	Risk-Based Decision is a decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment and processes. The type of information taken into account when making a risk-based decision may change based on life cycle phase and decision is made taking entire posture of the system into account. Some examples of information taken into account are formal and informal risk assessments, risk analysis, assessments, recommended risk mitigation strategies, and business impact. (This list is not intended to be all inclusive)
SA	System Administrator
SAMI	Sources and Methods Information
SHA	Secure Hash Algorithm is a hash algorithm with the property that it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. (FIPS 180-4)
SIEM	Security Information and Event Management server is Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedures
SP	Special Publications
SRG	Security Requirements Guide
STIG	Security Technical Implementation Guide
Syslog	A protocol that specifies a general log entry format and a log entry transport mechanism.

Exhibit 10.8.63-2 (Cont. 3) (07-24-2023)
Terms and Acronyms

TCP	Transmission Control Protocol is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other.
TD P	Treasury Directive Publication
UEM	Unified Endpoint Management
UNS	User and Network Services
Vendor	Vendors are commercial suppliers of software or hardware (NISTIR 4734) More specifically, vendors create or manufacture products for government organizations or contractors.

Exhibit 10.8.63-3 (07-24-2023)
Related Resources

Office of Management and Budget (OMB) Memoranda

- M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, August 27, 2021

Other Federal Guidance

- National Archives and Records Administration's (NARA) Universal Requirements for Electronic Systems, April 2020

IRS Publications

- IRM 115.6, *Records and Information Management, Managing Electronic Records*
- IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*
- IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*
- IRM 10.8.50, *Information Technology (IT) Security, Servicewide Security Patch Management Policy*

Department of the Treasury Publications

- Treasury Directive Publication (TD P) 85-01 Version 3.1.3, *Treasury Information Technology (IT) Security Program*, February 28, 2022

National Institute of Standards and Technology (NIST) Publications

- NIST FIPS 199, *Standards for Security Categorization of Federal Information and Systems*
- NIST FIPS 200, *Minimum Security Requirements for Federal Information and Systems*
- NIST SP 800-37 Rev 2, *Risk Management Framework for Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, September 20, 2018
- NIST SP 800-53 Rev 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, December 10, 2020
- NIST SP 800-53A Rev 5, *Assessing Security and Privacy Controls in Federal Systems and Organizations*, August 3, 2021
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, December 10, 2020
- NIST SP 800-190, *Application Container Security Guide*, September 25, 2017

Defense Information Systems Agency (DISA) Publications

- DISA *Central Log Server SRG - Ver 2, Rel 2*, October 27, 2022
- STIGs are used as a basis for producing IRS Security Requirements Checklists. The security checklists are updated as DISA releases updated guidance and are posted on the IRS Security Requirements Checklists SharePoint site. The DISA version and release for each guide is contained within each checklist. Refer to the Security Requirements Checklists exhibit for additional information.
- DISA security guides are available at: *https://public.cyber.mil/stigs/*.

Center for Internet Security Publications

- CIS Benchmarks are used as a basis for producing IRS Security Requirements Checklists. The security checklists are updated as CIS releases updated guidance and are posted in the IRS

Exhibit 10.8.63-3 (Cont. 1) (07-24-2023)
Related Resources

Security Control Exhibit SharePoint site. The CIS version for each benchmark is contained within each checklist. Refer to the Security Requirements Checklists exhibit for additional information.

- CIS benchmarks are available at: *https://www.cisecurity.org/cis-benchmarks/*.

Exhibit 10.8.63-4 (07-24-2023)
Implementation and Centralized Access Requirements

The following tables define the requirements necessary to meet each EL level. (OMB M-21-31)

Table 1: 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 Exhibit 10.8.63-5.
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 address5 or other unique identifier) ***Note:*** All hosts should be configured to have MAC randomization turned off. Where possible, this configuration should be maintained automatically. • 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 ***Note:*** Software developed by agencies or by contractors on behalf of agencies must log unique event identifiers for each event in accordance with these requirements.

Exhibit 10.8.63-4 (Cont. 1) (07-24-2023)
Implementation and Centralized Access 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. • 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 at: *https://www.nist.gov/pml/time-and-frequency-division/time-services/nist-authenticated-ntp-service*. Public, unauthenticated, and unencrypted NTP pools shall only be used as an option of last resort, and only for as long as needed n leveraging other options. ***Note:*** 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.
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 and on an automated basis, to centralized systems responsible for security, information, and event monitoring (SIEM); bulk storage; and other 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. ***Note:*** 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.

Exhibit 10.8.63-4 (Cont. 2) (07-24-2023)
Implementation and Centralized Access Requirements

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 Exhibit 10.8.63-5, 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.

Exhibit 10.8.63-4 (Cont. 3) (07-24-2023)
Implementation and Centralized Access Requirements

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 3, 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 3, 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 2: 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 Exhibit 10.8.63-5.
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.

Exhibit 10.8.63-4 (Cont. 4) (07-24-2023)
Implementation and Centralized Access Requirements

Inspection of Encrypted Data	Federal agencies shall retain and store in cleartext form the data or metadata from Exhibit 10.8.63-5 that is collected in their environment. If agencies perform full traffic inspection through active proxies, they should log additional available fields as described in Exhibit 10.8.63-5 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 3: 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 Exhibit 10.8.63-5.
Logging Orchestration, Automation, and Response – Finalizing Implementation	Agencies shall finalize and implement automated hunt and incident response playbooks. Federal agencies shall also provide any updates to 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 Monitoring – early detection of malicious behavior. This technology leverages Finalizing machine learning and artificial intelligence techniques to detect Implementation 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

Exhibit 10.8.63-4 (Cont. 5) (07-24-2023)
Implementation and Centralized Access Requirements

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 (Reference NIST SP 800-190, Application Container Security Guide).
Advanced Centralized Access	Required Logs across all criticality levels shall be accessible to the highest-level security operations at the head of each agency.

Exhibit 10.8.63-5 (07-24-2023)
Logging Requirements – Technical Details

The following tables provide the technical details for logging requirements. (OMB M-21-31)

Note: Exceptions to the requirements are set below:
i. Full packet capture data is required to be stored for only 72 hours.
ii. The retention periods prescribed below are minimum values; data may be retained for longer periods if appropriate.

Table 4: Logging Requirements – Technical Details

Term	Description
Log Category	This column describes the various log categories from which logging data can be sourced. The tables in Exhibit 10.8.63-5 are organized by log criticality 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.

Exhibit 10.8.63-5 (Cont. 1) (07-24-2023)
Logging Requirements – Technical Details

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.

a. Criticality = 0

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

Exhibit 10.8.63-5 (Cont. 2) (07-24-2023)
Logging Requirements – Technical Details

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
	• Isolate, Monitor, Record, Audit Privilege Sessions
	• Control Privileged Actions
	  • Commands
	  • Tasks
	• Track Privilege Escalation and Delegation
	• Monitor, Alert and Respond to Anomalous Behaviors/Activities
		Log
		
		Script
			0	12 Months Active Storage
				
				18 Months Cold Data Storage

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

Exhibit 10.8.63-5 (Cont. 3) (07-24-2023)
Logging Requirements – Technical Details

Network Device Infrastructure	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 Infrastructure	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 Infrastructure	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

Exhibit 10.8.63-5 (Cont. 4) (07-24-2023)
Logging Requirements – Technical Details

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	Log File Config	0	12 Months Active Storage 18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 5) (07-24-2023)
Logging Requirements – Technical Details

Network Device Infrastructure (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 o Hostname o IP Address and Port o MAC • Destination o Hostname o IP Address and Port o 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

Exhibit 10.8.63-5 (Cont. 6) (07-24-2023)
Logging Requirements – Technical Details

Network Device Infrastructure	Proxies and Web Content Filters • Policy Updates • Software Updates	Log	0	12 Months Active Storage 18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 7) (07-24-2023)
Logging Requirements – Technical Details

Proxies and Web Content Filters • Policy Updates • Software Updates	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 • 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	Log	0	12 Months Active Storage 18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 8) (07-24-2023)
Logging Requirements – Technical Details

	• 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			

Exhibit 10.8.63-5 (Cont. 9) (07-24-2023)
Logging Requirements – Technical Details

Operating Systems Windows Infrastructure 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 File Access • Transfer of Data to External Media or Remote Hosts Host Network Communications • Listening Network Port and IP Address • Active Network Communication with Other Hosts Powershell Execution Commands WMI Events Command-Line Interface (CLI) Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware • Version • Created Date • Installed Date • Manufacturer	Log	0	12 Months Active Storage 18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 10) (07-24-2023)
Logging Requirements – Technical Details

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 • 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	Log	0	12 Months Active Storage 18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 11) (07-24-2023)
Logging Requirements – Technical Details

	• 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			

Exhibit 10.8.63-5 (Cont. 12) (07-24-2023)
Logging Requirements – Technical Details

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 • Active Network Communication with Other Hosts Command-Line Interface (CLI) Security Enhanced Linux (SELinux) AppArmor or Equivalent • Warning Logs • Violation Logs	Log	0	12 Months Active Storage 18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 13) (07-24-2023)
Logging Requirements – Technical Details

	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			

Exhibit 10.8.63-5 (Cont. 14) (07-24-2023)
Logging Requirements – Technical Details

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 Environments (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

Exhibit 10.8.63-5 (Cont. 15) (07-24-2023)
Logging Requirements – Technical Details

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 • Usage Logs • Storage Logs • Data Access Logs For Organizational and Default Configuration Settings Enable: • Admin Read • Data Read • Data Write	Log	0	12 Months Active Storage 18 Months Cold Data Storage

b. Criticality = 1

Exhibit 10.8.63-5 (Cont. 16) (07-24-2023)
Logging Requirements – Technical Details

Log Category	Required Data	Format	Criticality	Retention Period
System Configuration and Performance	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 Configuration and Performance	Endpoint Detection & Response (EDR)	Log	1	12 Months Active Storage 18 Months Cold Data Storage
System Configuration and Performance	Configuration Changes • Management Action (Success/Failure) • Admin Login (Success/Failure)	Log	1	12 Months Active Storage 18 Months Cold Data Storage

Authentication and Authorization
Note: These requirements are general requirements that apply to systems and applications that are not specified in this document.
	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

Exhibit 10.8.63-5 (Cont. 17) (07-24-2023)
Logging Requirements – Technical Details

Authentication and Authorization ***Note:*** These requirements are general requirements that apply to systems and applications that are not specified in this document.	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
	• Identity or (Hash) Identifier of the File(s)
	• Description of the Action Taken (Clean, Quarantine, Delete)
	• Signature Updates
		Log
		
		Email Attachments
			1	12 Months Active Storage
				
				18 Months Cold Data Storage

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

Exhibit 10.8.63-5 (Cont. 18) (07-24-2023)
Logging Requirements – Technical Details

Network Device Infrastructure	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 Infrastructure (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

Exhibit 10.8.63-5 (Cont. 19) (07-24-2023)
Logging Requirements – Technical Details

Network Device Infrastructure (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

Exhibit 10.8.63-5 (Cont. 20) (07-24-2023)
Logging Requirements – Technical Details

Network Device Infrastructure (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)
	• Change in Status of Connections / Tunnel Status
	• VPN Certificate Status Validation
		Log	1	12 Months Active Storage
				
				18 Months Cold Data Storage

PKI Infrastructure	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

Exhibit 10.8.63-5 (Cont. 21) (07-24-2023)
Logging Requirements – Technical Details

Vulnerability Assessments	• Date and Time • Hostname, IP Address, and OS Active Assessment Version • Open Ports • Installed Applications • Version of Installed Applications • Vulnerabilities Listed in Installed Applications • Source of Vulnerability and Severity	Log ***Note:*** Logs are kept for ALL assessments, even if there are 0 vulnerabilities identified during the assessment.	1	12 Months Active Storage 18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 22) (07-24-2023)
Logging Requirements – Technical Details

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

Exhibit 10.8.63-5 (Cont. 23) (07-24-2023)
Logging Requirements – Technical Details

Application Level	Web Applications • URL • Headers • HTTP Methods -Request with Body of Data • This data shall be evaluated to ensure proper protections are in place to encrypt the data at rest and in transit. Tools shall be accredited to handle sensitive data and proper oversight controls shall be implemented to look for signs of inappropriate data usage. • HTTP Response with Body of Data	Log Log and PCAP of Plaintext HTTP Request and Response with Data	1	12 Months Active Storage 18 Months Cold Data Storage
Application Level	Web Applications • Database Queries • Response Codes	Log	1	12 Months Active Storage 18 Months Cold Data Storage
Application Level	Web Applications • Processes • Applications	Log	1	12 Months Active Storage 18 Months Cold Data Storage
Application Level	Web Applications • Configuration • Version	Log	1	12 Months Active Storage 18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 24) (07-24-2023)
Logging Requirements – Technical Details

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

Exhibit 10.8.63-5 (Cont. 25) (07-24-2023)
Logging Requirements – Technical Details

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 Crypto-graphic Capabilities (e.g., Trusted Boot Process) • Certificate Validation Failure (Defined in MDM Server Pro-tection Profile) • Alerts from Agent to Server Defined MDM Agent Protection Profile	Log	1	12 Months Active Storage 18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 26) (07-24-2023)
Logging Requirements – Technical Details

Mobile (Smartphones 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., SHA256) • Running Apps and Processes Device Policy Settings • Enrollment Policies • Policies Successfully/ Unsuccessfully Applied • 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	Log	1	12 Months Active Storage 18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 27) (07-24-2023)
Logging Requirements – Technical Details

	• 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	Log Manual Log Entry	1	12 Months Active Storage 18 Months Cold Data Storage

c. Criticality = 2

Log Category	Required Data	Format	Criticality	Retention Period

Exhibit 10.8.63-5 (Cont. 28) (07-24-2023)
Logging Requirements – Technical Details

System Configuration and Performance	System Status • Resource Utilization • Performance	Log Database Recored Script	2	12 Months Active Storage 18 Months Cold Data Storage

Email Filtering, Spam, and Phishing	Raw and Metadata -Filtering Events15
	• 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
	
	Note: 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.
		Log
		
		Email Attachments
			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 Attachments
			2	12 Months Active Storage
				
				18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 29) (07-24-2023)
Logging Requirements – Technical Details

Network Traffic	Full Packet Capture Data • Decrypted Plaintext • Cleartext	Packet Capture	2	12 Months Active Storage 18 Months Cold Data Storage

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

Exhibit 10.8.63-5 (Cont. 30) (07-24-2023)
Logging Requirements – Technical Details

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

Exhibit 10.8.63-5 (Cont. 31) (07-24-2023)
Logging Requirements – Technical Details

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 Dashboard	2	12 Months Active Storage 18 Months Cold Data Storage

Exhibit 10.8.63-5 (Cont. 32) (07-24-2023)
Logging Requirements – Technical Details

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
	  • Transfer of Data to External Media
	• Powershell Execution Commands
	• WMI Events
	• Registry Access
	• Command-Line Interface (CLI)
		Log	2	12 Months Active Storage
				
				18 Months Cold Data Storage

d. Criticality = 3

Log Category	Required Data	Format	Criticality	Retention Period

Exhibit 10.8.63-5 (Cont. 33) (07-24-2023)
Logging Requirements – Technical Details

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) ***Note:*** See DISA's zOS Mainframe STIG for log configuration guidance • Output from Integrated Intrusion Detection Services	Log	3	12 Months Active Storage 18 Months Cold Data Storage
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	12 Months Active Storage 18 Months Cold Data Storage