



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.63

MAY 15, 2025

EFFECTIVE DATE

(05-15-2025)

PURPOSE

- (1) This transmits revised IRM 10.8.63, *Information Technology (IT) Security, Central Log Server Security Policy*.

MATERIAL CHANGES

- (1) Throughout the IRM:
 - Changed instances of "shall" to "must" where appropriate.
 - Changed instances of "this policy" and "this manual" to "this IRM".
 - Added a leading zero to single digit NIST controls. Example: AC-2 is now AC-02.
 - Revised source citation and baseline indicator formatting.
 - Updated references to IRM 10.8.1 to include a reference to IRM 10.8.24.
- (2) 10.8.63.1 Program Scope and Objectives:
 - (1)a) Updated title of IRM 10.8.1.
 - (1)b) Added language indicating that the IRM is subordinate to IRM 10.8.24 for off-premises cloud deployments.
 - (3)c) Added language indicator applicability of guidance found within the IRM.
 - (4) Added CIO acronym.
 - (5) Updated Cybersecurity Threat Response and Remediation title.
- (3) 10.8.63.1.3 Roles and Responsibilities: Added reference to subsection where DNS specific roles and responsibilities are located.
- (4) 10.8.63.1.4 Program Management and Review: (2) Added program management language.
- (5) 10.8.63.1.5 Program Controls:
 - (3) Removed duplicate language.
 - (4) Removed duplicate language.
 - (5) Added language defining FIPS 199 impact-level and overlay indicators, and source citation formatting used throughout the IRM.
 - (6) Added table showing formatting examples.
- (6) 10.8.63.1.6 Terms and Acronyms: Added exhibit title.
- (7) 10.8.63.1.7 Related Resources: Added exhibit title.
- (8) 10.8.63.2 Risk Acceptance and Risk-Based Decisions (RBDs):
 - (2) Updated SRM document title.
 - (2) Note: Updated URL.
- (9) 10.8.63.3 IT Roles and Responsibilities: New subsection added for where DNS specific roles and responsibilities are located.
- (10) 10.8.63.4 IT Security Controls: (3) Subsection title added.

- (11) 10.8.63.4.1.1 AC-02 Account Management:
- (5) Incorporated SRG requirement SRG-APP-000163-AU-002470 from IA-4 Identifier Management subsection (now removed).
 - (10) Added new SRG requirement SRG-APP-000705-AU-000110.
- (12) 10.8.63.4.2: Updated subsection title to align with NIST SP 800-53 Rev5.
- (13) 10.8.63.4.3.5 AU-06 Audit Record Review, Analysis, and Reporting: (2) Added new SRG requirement SRG-APP-000745-AU-000120.
- (14) 10.8.63.4.3.6 AU-07 Audit Record Reduction and Report Generation:
- (12) Added new SRG requirement SRG-APP-000750-AU-000130.
 - (13) Added new SRG requirement SRG-APP-000755-AU-000140.
 - (14) Added new SRG requirement SRG-APP-000760-AU-000150.
 - (15) Added new SRG requirement SRG-APP-000765-AU-000160.
 - (16) Added new SRG requirement SRG-APP-000770-AU-000170.
 - (17) Added new SRG requirement SRG-APP-000775-AU-000180.
 - (18) Added new SRG requirement SRG-APP-000780-AU-000190.
 - (19) Added new SRG requirement SRG-APP-000785-AU-000200.
 - (20) Added new SRG requirement SRG-APP-000790-AU-000210.
- (15) 10.8.63.4.3.8 AU-09 Protection of Audit Information: (8) Added new SRG requirement SRG-APP-000795-AU-000220.
- (16) 10.8.63.4.3.11 AU-12 Audit Record Generation:
- Updated subsection title to align with NIST SP 800-53 Rev5.
 - (4) Removed SRG-APP-000088-AU-000040 due to the requirement being removed from the DISA Central Log Server SRG with V3R1.
 - (9) Added new SRG requirement SRG-APP-000800-AU-000230.
- (17) 10.8.63.4.5 CM - Configuration Management: CM-04 title corrected.
- (18) 10.8.63.4.5.1 CM-05 Access Restrictions for Change:
- New subsection added.
 - (1) Added new SRG requirement SRG-APP-000805-AU-000240.
- (19) 10.8.63.4.5.4 CM-14 Signed Components:
- New subsection added.
 - (1) Added new SRG requirement SRG-APP-000810-AU-000250.
- (20) 10.8.63.4.7 IA - Identification and Authentication:
- (1) Added language directing the reader to IRM 10.8.1 and IRM 10.8.24.
 - IA-01 title updated.
 - IA-04 Identifier Management added to list.
 - IA-10 title updated.
 - IA-13 Identity Providers and Authorization Servers added to list.
- (21) 10.8.63.4.7.1 IA-02 Identification and Authentication (Organizational Users):
- (4) Corrected SRG-APP-000151-AU-002330 language to reflect local access restriction.
 - (9) Added new SRG requirement SRG-APP-000815-AU-000260.
 - (10) Added new SRG requirement SRG-APP-000825-AU-000280.

- (22) Old 10.8.63.4.7.2 IA-4 Identifier Management:
- Subsection removed.
 - SRG requirement SRG-APP-000163-AU-002470 relocated to 10.8.63.4.1.1 AC-02 Account Management subsection.
- (23) 10.8.63.4.7.3 IA-05 Authenticator Management:
- (16) Added new SRG requirement SRG-APP-000830-AU-000290.
 - (17) Added new SRG requirement SRG-APP-000835-AU-000300.
 - (18) Added new SRG requirement SRG-APP-000840-AU-000310.
 - (19) Added new SRG requirement SRG-APP-000845-AU-000320.
 - (20) Added new SRG requirement SRG-APP-000855-AU-000340.
 - (21) Added new SRG requirement SRG-APP-000860-AU-000350.
 - (22) Added new SRG requirement SRG-APP-000865-AU-000360.
 - (23) Added new SRG requirement SRG-APP-000875-AU-000380.
- (24) 10.8.63.4.18 SC – System and Communications Protection:
- Updated SC-01 title to be Policy and Procedures.
 - Updated SC-16 title to be Transmission of Security and Privacy Attributes.
 - Removed SC-17 Public Key Infrastructure (PKI) Certificates from the list.
 - Removed SC-28 Protection of Information at Rest from the list.
 - Updated SC-35 title to be External Malicious Code Identifier.
 - Removed SC-45 System Time Synchronization from the list.
- (25) 10.8.63.4.18.3 SC-17 Public Key Infrastructure (PKI) Certificates:
- New subsection added.
 - (1) Added new SRG requirement SRG-APP-000910-AU-000390.
- (26) 10.8.63.4.18.5 SC-28 Protection of Information at Rest:
- New subsection added.
 - (1) Added new SRG requirement SRG-APP-000915-AU-000400.
- (27) 10.8.63.4.18.6 SC-45 System Time Synchronization:
- New subsection added.
 - (1) Added new SRG requirement SRG-APP-000920-AU-000410.
 - (2) Added new SRG requirement SRG-APP-000925-AU-000420.
- (28) Exhibit 10.8.63-1 Security Requirements Checklists:
- 2) Updated URL.
 - 3) Updated IRM 10.8.50 title.
- (29) Exhibit 10.8.63-2 Terms and Acronyms:
- Added the following Acronyms: ACL, API, BGP, BIOS, CAC, CAVP, CHMOD, CMVP, CIO, CIP, CISA, CLI, CNSSI, COTS, CRUD, CSW, DLP, DNS, EDR, ELM, ESSID, FBI, FTP, GMT, GPS, HTTP, HVA, IDS, InTC, IP, IPS, IPv4, IPv6, IRS, ISO, LDAP, MAC, MITM, NARA, NDR, NFS, NRT, NTA, OAuth, OS, RDP, S3, SA&A, SELinux, SMB, SNI, SOAR, SOC, SRM, SSL, SSO, UEFI, URL, UTC, VMS, VNet, VPC, W3C, WAF, and Wi-Fi.
 - Removed the following Acronyms no longer in the IRM: ISSO.
 - Added the following terms: AppArmor, De-NAT IP Address, External System Service Provider, NSA-Approved Cryptography, Runas, Sudo, and Zulu Time.

- Revised the following terms: Application, Cybersecurity, FIPS, FISMA, and PKI.
- Removed the following terms no longer in the IRM: Outsourcing Provider.

(30) Exhibit 10.8.63-3 Related Resources:

- Office of Management and Budget (OMB) Memoranda relocated to Other Publications area.
- Corrected reference to IRM 1.15.6.
- Added IRM 10.5.1, Privacy Policy.
- Added IRM 10.8.24, Cloud Computing Security Policy.
- Added FIPS 180-4, Secure Hash Standard (SHS).
- Removed NIST SP 800-37 Revision 2.
- Added FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors.
- Removed NIST SP 800-53A Revision 5.
- Removed NIST SP 800-53B.
- Added NIST SP 800-63-3, Digital Identity Guidelines.
- Added NIST SP 800-70 Revision 4, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers.
- Added NIST SP 800-92, Guide to Computer Security Log Management.
- Added NIST SP 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.
- Added NIST SP 800-171 Revision 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
- Added NIST IR 4734, Foundations of a Security Policy for Use of the National Research and Educational Network.
- Replaced DISA Central Log Server SRG Version 2 Release 2 with Version 3 Release 3.
- Removed duplicate STIG and checklist language.
- Removed Center for Internet Security Publications due to the publications aren't used for this IRM.
- Added Other Publications area.
- Added CNSSI 4009, Committee on National Security Systems (CNSS) Glossary.
- Added NARA, Universal Requirements for Electronic Systems.
- Added Title 44 U.S. Code Section 3551, Purposes.

(31) Exhibit 10.8.63-5 Logging Requirements – Technical Details:

- Network Device Infrastructure - Proxies and Web Content Filters: Added Source and Destination attributes.
- Table a) Criticality = 0, Log Category = Operating System Windows Infrastructure and Operating Systems: Added "System Configuration" to Required Data column.
- Table a) Criticality = 0, Log Category = Operating System Windows Infrastructure and Operating Systems: Added "Registry Access" to Required Data column.

(32) Editorial changes (including grammar, spelling and minor clarifications) were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.8.63 dated July 27, 2023. This IRM supplements IRM 10.8.1, *Security Policy*; IRM 10.8.2, *IT Security Roles and Responsibilities*, and IRM 10.8.24, **Cloud Computing Security Policy**.

AUDIENCE

All personnel responsible for overseeing, managing, and implementing centralized log server security for IRS information systems.

Rajiv Uppal
Chief Information Officer

Central Log Server Security Policy

10.8.63.1 Program Scope and Objectives (SPDER)

- 10.8.63.1.1 Background
- 10.8.63.1.2 Authority
- 10.8.63.1.3 Roles and Responsibilities
- 10.8.63.1.4 Program Management and Review
- 10.8.63.1.5 Program Controls
- 10.8.63.1.6 Terms and Acronyms
- 10.8.63.1.7 Related Resources
- 10.8.63.2 Risk Acceptance and Risk-Based Decisions (RBDs)
- 10.8.63.3 IT Roles and Responsibilities
- 10.8.63.4 IT Security Controls

[illegible]

[illegible]

#

- | | |
|-----------|--|
| 10.8.63-2 | Terms and Acronyms |
| 10.8.63-3 | Related Resources |
| 10.8.63-4 | Implementation and Centralized Access Requirements |
| 10.8.63-5 | Logging Requirements – Technical Details |

10.8.63.1
(05-15-2025)
Program Scope and Objectives (SPDER)

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of centralized log servers within the IRS.
 - a. This IRM is subordinate to IRM 10.8.1, *Security Policy* and augments the existing requirements identified within IRM 10.8.1, as they relate to IRS centralized logging server security for on-premises systems, including on-premises cloud deployments.
 - b. This IRM is subordinate to IRM 10.8.24, *Cloud Computing Security Policy*, and augments the existing requirements identified within IRM 10.8.24, as they relate to IRS centralized log server security for off-premises cloud deployments.
- (2) **Program Purpose:** Develop and publish security policies to protect the IRS against potential security threats, risks, and vulnerabilities to ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this IRM apply to:
 - a. All offices, business units, operating units, and functional units within the IRS.
 - b. IRS personnel and organizations having contractual arrangements with the IRS, including employees, contractors, vendors and external system service providers, which use or operate systems that store, process, or transmit IRS information or connect to an IRS network or system.
 - c. All systems regardless of their National Institute of Standards and Technology (NIST) impact-level (i.e., Low, Moderate, High), unless a requirement indicates differently.
- (4) **Policy Owner:** Chief Information Officer (CIO)
- (5) **Program Owner:** Cybersecurity, Cybersecurity Threat Response and Remediation
- (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 IRM 10.8 Information Technology (IT) Security series for IRS IT Cybersecurity.

10.8.63.1.2
(05-15-2025)
Authority

- (1) All IRS systems and applications are required to comply with executive orders (EOs), Office of Management and Budget (OMB), Federal Information Security Modernization Act of 2014 (FISMA), NIST, Cybersecurity and Infrastructure Security Agency (CISA), National Archives and Records Administration (NARA), Department of the Treasury, and IRS guidelines as they apply.

10.8.63.1.3
(05-15-2025)
Roles and Responsibilities

- (1) The IRS must implement security roles in accordance with federal laws and IT security guidelines (e.g., FISMA, NIST, OMB) that are appropriate for their specific operations and missions. The roles and responsibilities are defined in IRM 10.8.2 , *IT Security Roles and Responsibilities*.
- (2) Supplemental roles and responsibilities specific to the implementation of application servers (if any) are located in IRM 10.8.63.3, *IT Roles and Responsibilities*, subsection of this IRM.

10.8.63.1.4
(05-15-2025)
Program Management and Review

- (1) The IRS security policy program establishes a framework of controls to ensure the inclusion of security into the IRS IT environment. This framework of security controls is provided through the issuance of security policies via the IRM 10.8 series and the development of technology specific security requirements checklists. Stakeholders are notified when revisions to the security policies and security requirements checklists are made.
- (2) It is the policy of the IRS to:
- a. Establish and manage an information security program within its organizations. This IRM provides uniform policies and guidance to be used by each organization.
 - b. Protect all IT resources belonging to, or used by, the IRS at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that IT resource.
 - c. Protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, OMB guidance, Treasury Directives (TDs), NIST publications, NARA guidance, other regulatory guidance, and best practice methodologies.
 - d. Use best practice methodologies (such as Capability Maturity Model Integration (CMMI), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.63.1.5
(05-15-2025)
Program Controls

- (1) Each IRM in the 10.8 series is assigned an author who reviews the IRM 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 requirements 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 requirements checklists that have recently been revised or are in the revision process.
- (3) For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *Classified National Security Information (CNSI)*, for additional guidance on protecting classified information.
- (4) This IRM establishes the minimum baseline security policy and requirements for all IRS centralized log servers.
- (5) To define a security policy baseline for IRS systems, risk impact level and overlay designators may be assigned to a requirement and appear at the end of it in brackets, which will help identify if the requirement applies to a system:

Note: When there are sub-parts (e.g., a, b, i, ii) to a primary requirement and a designator is indicated for the primary requirement but not the sub-parts, the designator indicated for the primary applies to the sub-parts as well.

- a. A federal information processing standards (FIPS) 199 security impact-level designator may be assigned to each requirement. This designator indicates that the requirement only applies to systems categorized at that FIPS 199 impact-level, thus establishing a baseline for each level.

Example: A requirement with an indicator of “H” indicates the requirement only applies to systems categorized as FIPS 199 impact-level HIGH.

- b. Controls designated as program-level controls are identified with an “O” indicator. The following apply for controls designated as program-level requirements:
 - i. Implemented at the organization level;
 - ii. Not directed at individual systems;
 - iii. Independent of any system impact level; and
 - iv. Not associated with security control baselines.

Note: This indicator is in place of the FIPS 199 designators previously defined.

- c. Control identified as part of the privacy control baseline are identified with a “(P)” indicator.
- d. Controls designated as a critical infrastructure protection (CIP) overlay control are identified with a “CIP” indicator. Systems designated as cyber critical infrastructure assets must implement controls identified as CIP overlay controls.
 - i. The critical infrastructure control overlay” must be applied to all components within the designated cyber critical infrastructure asset system’s security boundary.

Note: Information systems normally consist of components (servers, routers, batch processing routines, mainframes, etc.) that when combined allow the overall system to perform its intended function. The intent is to increase the trustworthiness and resiliency of the overall system by applying the control overlay to all the components of the designated system, where applicable. It is understood that security controls are applicable only to information system components that provide or support the capability addressed by the controls. Document the implementation accordingly.

Note: CIP overlay controls may be tailored as long as the following criteria is met:

1. The authorizing official (AO), in coordination with the system and organizational officials determines that a control in the overlay is not to be implemented (also referred to as “tailoring-out”) on a designated cyber critical infrastructure asset; and
2. The associated documentation for this risk-based decision not to implement must be submitted to the Department Cyber CIP Program Manager and the Departmental CISO for review and approval.

- e. Controls designated as a high value asset (HVA) overlay control are identified with an “HVA” indicator. Systems designated as an HVA must implement security controls identified as HVA overlay controls.

Note: The PM and PT family of controls in the CISA government-wide baseline are excluded from the IRM 10.8.24 baseline.

Note: The HVA control overlay is defined by CISA.

- f. Controls designated as a critical software (CSW) overlay control are identified with a “CSW” indicator. Software designated as critical software and platforms hosting critical software must implement security controls identified as CSW overlay controls. [NIST: NIST Security Measures for EO-Critical Software Use]

Note: Security controls identified as CSW align with the security measures defined by NIST.

Indicator	Applicability
(L)	Applies to systems categorized as FIPS 199 Impact-level LOW.
(M)	Applies to systems categorized as FIPS 199 Impact-level MEDIUM.
(H)	Applies to systems categorized as FIPS 199 Impact-level HIGH.
(CIP)	Overlay - Applies to systems identified as Cyber Critical Infrastructure.
(HVA)	Overlay - Applies to systems identified as Cyber High Value Assets.
(P)	Privacy Baseline Controls

Indicator	Applicability
(O)	Program-level Controls (i.e., Program Management (PM))
(CSW)	Overlay - Applies to software identified as Critical Software and systems hosting Critical Software.

- (6) In an effort to provide an authoritative source for a requirement, a citation may be provided at the end of a requirement within brackets. If a NIST impact-level baseline (i.e., L, M, H) or control overlay (i.e., CIP, HVA) applies to a requirement, they would be provided at the end of a requirement within brackets also. The citations, baselines, and overlays are broken down into two parts: the first part is a generic identifier, such as NIST, DISA, Baseline, Overlay, etc.; the second part identifies the specific source, baseline or overlay that applies. Below are some examples of how a citation, baseline, and/or overlay may appear for a particular type of source:

a. Citations

Citation	Example
NIST Control	NIST Control [NIST: SP 800-53, AC-02]
Treasury Control	Treasury Control [Treasury: TD P 85-01, AC-03_T.002]
Treasury Publication	Treasury Publication [Treasury: TD P 15-71]
Federal	Federal [Federal: P.L. 113-283]
U.S. Code	U.S. Code [USC: 44 USC 3551]
Executive Order	Executive Order [EO: 14028]
OMB Memorandum	OMB Memorandum [OMB: M-22-09]
CISA Directive	CISA [CISA: BOD-23-01]
NIST Publication	[NIST: SP 800-40]
DISA STIG/SRG	[DISA: SRG-APP-000516-NDM-000350]
IRS Defined with no business unit source	[IRS: IRS-defined]
IRS Defined with CSIRC as source	[CSIRC: IRS-defined]

b. Baseline

NIST Baseline	[Baseline: P, L, M, H, O]
---------------	---------------------------

c. Overlay

Control Overlay

[Overlay: CIP, HVA, CSW]

Example: How a source, baseline, overlay could appear at the end of a requirement: [NIST: SP 800-53, SA-15 | Baseline: M, H | Overlay: HVA].

Note: Citations correlate to a reference listed in Exhibit 10.8.63-3 Exhibit 10.8.63-3, Related Resources.

Note: The citation, baseline, and overlay are formatted to be simple enough for manual identification while being distinct enough for automated detection and extraction. This is intended to allow for easy identification and parsing by applications (manual or automated), using distinct patterns.

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

10.8.63.1.6
(05-15-2025)

Terms and Acronyms

- (1) Refer to Exhibit 10.8.63-2, *Terms and Acronyms*, for a list of terms, acronyms, and definitions.

10.8.63.1.7
(05-15-2025)

Related Resources

- (1) In addition to federal guidance cited throughout this IRM, this IRM incorporates IRS-defined policy, regulatory and mandated guidance, and policy from other sources. Refer to Exhibit 10.8.63-3, Related Resources, for a list of related resources and references.

10.8.63.2
(05-15-2025)

Risk Acceptance and Risk-Based Decisions (RBDs)

- (1) Any exception to this IRM requires the AO to make a risk acceptance decision.
- (2) Users must submit risk-based decision (RBD) requests in accordance with Cybersecurity's Security Risk Management (SRM) risk acceptance process documented in the Request for Risk Acceptance and Risk Based Decision Standard Operating Procedures (SOP).

Note: Users can access the RBD documentation in the FISMA Doc Library on the *Enterprise FISMA Compliance (EFC)* site.

- (3) Refer to IRM 10.8.1 for additional guidance on risk acceptance and RBDs.

10.8.63.3
(05-15-2025)

IT Roles and Responsibilities

- (1) This IRM does not contain supplemental roles and responsibilities specific to the implementation of centralized log servers.

10.8.63.4
(07-24-2023)

IT Security Controls

- (1) The security controls in this IRM supplement the requirements found in IRM 10.8.1 or IRM 10.8.24 (as applicable).
- a. Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) 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 IRM 10.8.63.2, *Risk Acceptance and Risk-Based Decisions (RBDs)*, subsection for additional guidance.

#

```
## ## ##
## ##
## ##
## ## ## ## ##
## ## ## ## ## ##
## ##
## ##
## ## ## ## ## ##
## ##
## ## ## ## ##
## ## ##
```


#

#

#

#

#

#

#####

#

#

[illegible]

#

[illegible]

#

#

##

Exhibit 10.8.63-2 (05-15-2025)**Terms and Acronyms**

Term	Definition or Description
ACL	Access Control List – A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity. [CNSSI: 4009]
Application	A software program hosted by an information system. [CNSSI: 4009]
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. [CNSSI: 4009]
AO	Authorizing Official
API	Application Programming Interface
AppArmor	A Linux kernel security module that allows system administrators to restrict the capabilities of individual programs by creating specific security profiles, essentially acting as a sandbox to limit what resources an application can access, thus enhancing system security by preventing unauthorized access to sensitive data and mitigating potential vulnerabilities.
Authenticator	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. [CNSSI: 4009]
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
CAC	Common Access Card
CAVP	Cryptographic Algorithm Validation Program
CHMOD	The chmod, or change mode, command allows an administrator to set or modify a file's permissions.
CMVP	Cryptographic Module Validation Program
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CLI	Command Line Interface
Contractor	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.

Exhibit 10.8.63-2 (Cont. 1) (05-15-2025)

Terms and Acronyms

Term	Definition or Description
CNSSI	Committee on National Security Systems Instruction
COTS	Commercial Off the Shelf
CRUD	Create, Read, Update, and Delete
CSIRC	Computer Security Incident Response Center
CSW	Critical Software
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. [CNSSI: 4009]
De-NAT IP Address	The process of reversing a network address translation (NAT) operation, essentially taking a public IP address assigned by a NAT device and converting it back to the original private IP address of the internal device that initiated the connection, allowing for identification of the specific device within a network that sent the traffic.
DISA	Defense Information Systems Agency
DLP	Data Loss Prevention
DNS	Domain Name System
EA	Enterprise Architecture
EDR	Endpoint Detection & Response
EL	Event Logging
ELM	Enterprise Log Manager
EMM	Enterprise Mobility Management
EO	Executive Order
ESP	Enterprise Standards Profile
ESSID	Wi-Fi Extended Service Set Identifier
External System Service Provider	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. [CNSSI: 4009]
FBI	Federal Bureau of Investigation

Exhibit 10.8.63-2 (Cont. 2) (05-15-2025)

Terms and Acronyms

Term	Definition or Description
FIPS	Federal Information Processing Standards (FIPS) – A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability. [CNSSI: 4009]
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 <i>NSA-approved cryptography</i> . [CNSSI: 4009]
FISMA	The Federal Information Security Modernization of 2014 – Directs federal agencies to develop, document, and implement agency-wide programs to provide security for the information and systems that support the agency's operations and assets. This includes the security authorization and accreditation (SA&A) of IT systems that support digital authentication. [CNSSI: 4009]
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
GPS	Global Positioning System
HMAC	Hash Message Authentication Code – A message authentication code that uses a cryptographic key in conjunction with a hash function. [CNSSI: 4009]
HTTP	Hypertext Transfer Protocol
HVA	High Value Asset
IDS	Intrusion Detection System
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
InTC	Insider Threat Capability
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IRM	Internal Revenue Manual
IRS	Internal Revenue Service

Exhibit 10.8.63-2 (Cont. 3) (05-15-2025)**Terms and Acronyms**

Term	Definition or Description
ISO	International Organization for Standardization
KDF	Key Derivation Functions
LDAP	Lightweight Directory Access Protocol
Log	A record of the events occurring within an organization's systems and networks.
MAC	Media Access Control
MDM	Mobile Device Management
MFA	Multifactor Authentication – Authentication using two or more 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. [CNSSI: 4009]
MITM	Man-in-the-Middle
MTD	Mobile Threat Defense
NARA	National Archives and Records Administration
NDR	Network Detection and Response
NFS	Network File System
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.
NRT	Near Real Time
NSA-Approved Cryptography	Cryptography that consists of an approved algorithm, an implementation that has been approved for the protection of classified information and/or controlled unclassified information in a specific environment, and a supporting key management infrastructure. [CNSSI: 4009]
NTA	Network Traffic Analysis
NTP	Network Time Protocol – Used in networks of all types and sizes for time synchronization of servers, workstations, and other networked equipment. [CNSSI: 4009]
OAuth	Open Authorization
OMB	Office of Management and Budget
OS	Operating System
PCAP	Packet Capture
PIN	Personal Identification Number

Exhibit 10.8.63-2 (Cont. 4) (05-15-2025)**Terms and Acronyms**

Term	Definition or Description
PIV	Personal Identity Verification – 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 201-3. [CNSSI: 4009]
PKI	Public Key Infrastructure – The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates. [CNSSI: 4009]
RBD	Risk-Based Decision – 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)
RDP	Remote Desktop Protocol
Runas	A Windows command that allows a user to run a program or tool with the privileges of a different user account, essentially letting them execute a program “as” another user, including administrator level access, even if they are currently logged in with a standard user account; similar to the “sudo” command on Linux systems.
S3	Amazon S3
SA	System Administrator
SA&A	Security Authorization and Accreditation
SAMI	Sources and Methods Information
SELinux	Security-Enhanced Linux
SHA	Secure Hash Algorithm – 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. [CNSSI: 4009]
SIEM	Security Information and Event Management – An application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.

Exhibit 10.8.63-2 (Cont. 5) (05-15-2025)**Terms and Acronyms**

Term	Definition or Description
SMB	Server Message Block
SNI	Server Name Indication
SNMP	Simple Network Management Protocol
SOAR	Security, Orchestration, Automation, and Response
SOC	System on a chip
SOP	Standard Operating Procedures
SP	Special Publications
SRG	Security Requirements Guide
SRM	Security Risk Management
SSL	Secure Sockets Layer
SSO	System Security Officer
STIG	Security Technical Implementation Guide
Sudo	A command-line utility that allows users to run programs with elevated privileges, such as root privileges.
Syslog	A protocol that specifies a general log entry format and a log entry transport mechanism.
TCP	Transmission Control Protocol – 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
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
UNS	User and Network Services
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
Vendor	Commercial suppliers of software or hardware. More specifically, vendors create or manufacture products for government organizations or contractors. [NIST: IR 4734]
VMS	Vulnerability Management Service
VNet	Virtual Network
VPC	Virtual Private Cloud
W3C	World Wide Web Consortium

Exhibit 10.8.63-2 (Cont. 6) (05-15-2025)**Terms and Acronyms**

Term	Definition or Description
WAF	Web Application Firewall
Wi-Fi	Wireless Fidelity
Zulu Time	The military name of UTC and GMT

Exhibit 10.8.63-3 (05-15-2025)**Related Resources****IRS Publications**

- IRM 1.15.6, *Records and Information Management, Managing Electronic Records*.
- IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*.
- 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 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*.
- IRM 10.8.50, *Information Technology (IT) Security, Enterprise Incident, Vulnerability, and Security Patch Management Policy*.
- IRM 10.9.1, *National Security Information, Classified National Security Information (CNSI)*.

Department of the Treasury Publications

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

National Institute of Standards and Technology (NIST) Publications

- FIPS 180-4: Federal Information Processing Standards Publication 180-4, “*Secure Hash Standard (SHS)*,” issued August 2015.
- FIPS 199: Federal Information Processing Standards Publication 199, “*Standards for Security Categorization of Federal Information and Information Systems*,” issued February 2004.
- FIPS 200: Federal Information Processing Standards Publication 200, “*Minimum Security Requirements for Federal Information and Information Systems*,” issued March 2006.
- FIPS 201-3: Federal Information Processing Standards Publication 201-3, “*Personal Identity Verification (PIV) of Federal Employees and Contractors*,” issued January 2022.
- SP 800-53: NIST Special Publication 800-53 Revision 5.1.1, “*Security and Privacy Controls for Information Systems and Organizations*,” issued November 7, 2023.
- SP 800-63-3: NIST Special Publication 800-63-3, “*Digital Identity Guidelines*,” issued June 2017 (includes updates as of 3/2/2020).
- SP 800-70: NIST Special Publication 800-70 Revision 4, “*National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*,” issued February 2018.
- SP 800-92: NIST Special Publication 800-92, “*Guide to Computer Security Log Management*,” issued September 2006.
- SP 800-161: NIST Special Publication 800-161 Revision 1, “*Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*,” issued May 2022 (includes updates as of 11/01/2024).
- SP 800-171: NIST Special Publication 800-171 Revision 3, “*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*,” issued May 2024.
- SP 800-190: NIST Special Publication 800-190, “*Application Container Security Guide*,” issued September 25, 2017.
- IR 4734: NIST Internal Report 4734, “*Foundations of a Security Policy for Use of the National Research and Educational Network*,” issued February 1992.

Defense Information Systems Agency (DISA) Publications

- DISA Central Log Server SRG Version 3 Release 2, issued January 30, 2025.
- DISA security guides are available on the *DISA STIGs Document Library* site.

Other Publications

Exhibit 10.8.63-3 (Cont. 1) (05-15-2025)**Related Resources**

- CNSSI: 4009: Committee on National Security Systems Instruction, “*Committee on National Security Systems (CNSS) Glossary*,” issued March 2, 2022.
- NARA: National Archives and Records Administration’s (NARA) Universal Requirements for Electronic Systems, issued April 2020.
- OMB: M-21-31, Office of Management and Budget Memorandum 21-31, “*Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents*,” issued August 27, 2021.
- USC: 3553: Title 44 U.S. Code Section 3551, “*Purposes*,” issued December 18, 2014.

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	<p>At a minimum, agencies must ensure that each event log contains the following data, if applicable:</p> <ul style="list-style-type: none"> • Properly formatted and accurate timestamp (see below for Time Standard requirements) • Status code for the event type • Device identifier (MAC address or other unique identifier) <p>Note: All hosts should be configured to have MAC randomization turned off. Where possible, this configuration should be maintained automatically.</p> <ul style="list-style-type: none"> • Session/Transaction ID • Autonomous System Number • Source IP (Internet Protocol Version 4 (IPv4)) • Source IP (Internet Protocol Version 6 (IPv6)) • Destination IP (IPv4) • Destination IP (IPv6) • Status Code • Response Time • Additional headers (i.e., HTTP headers) • Where appropriate, the username or userID must be included or both • Where appropriate, the command executed must be included • Where possible, all data must be formatted as key-value-pairs allowing for easy extraction • Where possible, a unique event identifier must be included for event correlation; a unique event identifier must be defined per event type <p>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.</p>

Exhibit 10.8.63-4 (Cont. 1) (07-24-2023)**Implementation and Centralized Access Requirements**

Time Standard	<p>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 must 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.</p> <ul style="list-style-type: none"> • 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. <p>Agencies must use a global positioning system (GPS) master station clock as a baseline reference for timestamps used for logs and systems producing logs. If GPS reference is not possible, agencies must use <i>NIST's authenticated time service</i>. Public, unauthenticated, and unencrypted NTP pools must only be used as an option of last resort, and only for as long as needed in leveraging other options.</p> <p>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.</p>
Event Forwarding	<p>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 must forward all required logging data, in near real-time and on an automated basis, to centralized systems responsible for 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.</p> <p>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.</p>

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

Protecting and Validating Log Information	<p>To ensure data integrity, logging facilities and log information must be protected by cryptographic methods from tampering and unauthorized access. Agencies must protect and monitor the integrity of their logs and systems producing logs by:</p> <ul style="list-style-type: none"> • Verifying that event logging is enabled and active for system components. <ul style="list-style-type: none"> • Traps must be put in place to monitor these data streams for disruption. • These traps must 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 or 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 must 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: <ul style="list-style-type: none"> • Credentials • Privileges and security settings • Content • Core attributes and size • Hash values • Configuration values
Passive Domain Name System (DNS)	<p>Federal agencies must 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 must implement accompanying analytics that allow for rapid identification of the host that sourced each DNS query. This capability must be monitored and triaged. Federal agencies must 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.</p>

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

CISA and FBI Access Requirements	Agencies must provide logs and other relevant data to CISA and the Federal Bureau of Investigation (FBI) upon request, to the extent consistent with applicable law, including 44 U.S.C. 3553(l). Agencies must provide such data in a format and by means agreed upon by the agency, CISA, or the FBI, and must 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 must maintain and manage logs by leveraging the additional logging to develop automated hunt and incident response playbooks. Such playbooks must take advantage of security, orchestration, automation, and response (SOAR) capabilities. Agencies at EL1 stage must start planning on how to best implement SOAR capabilities in their environment. For additional implementation requirements, please see Table 3, <i>EL3 Advanced Requirements, Logging Orchestration, Automation, and Response – Finalizing Implementation</i> .
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 must start planning on how to best implement a user behavior analytics capability in their environment, leveraging the logging requirements, in order to 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, <i>EL3 Advanced Requirements, User Behavior Monitoring – Finalizing Implementation</i> .
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 must 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 levels 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 must provide a document detailing the structure (schema) for those logs to CISA. Agencies must refer to guidance from CISA in developing this documented schema. Federal agencies must also provide all updates to the schema to CISA no later than one business day after they are finalized. The schema and associated documentation must be published to <i>Data.gov</i> .

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

Inspection of Encrypted Data	Federal agencies must 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	<p>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 level 2 are retained, at a minimum, at component level.</p> <ul style="list-style-type: none"> 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 must be monitored and triaged by the component-level and top-level enterprise SOCs. The enterprise SOC must 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 must finalize and implement automated hunt and incident response playbooks. Federal agencies must 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	<p>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 must implement a user behavior analytics capability, leveraging the logging requirements, in order to identify potentially malicious or malicious activity. This capability must monitor all user and non-user accounts. This capability must 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:</p> <ul style="list-style-type: none"> 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 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 must 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, <i>Application Container Security Guide</i>).
Advanced Centralized Access	Required Logs across all criticality levels must be accessible to the highest-level security operations at the head of each agency.

Exhibit 10.8.63-5 (05-15-2025)**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	<p>This column describes the acceptable formats for the required data. See below for definitions of the various formats that can appear in this column.</p> <ul style="list-style-type: none"> • 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) (05-15-2025)**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, Guide to Computer Security Log Management , 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 <ul style="list-style-type: none"> Account creation Manage credential type <ul style="list-style-type: none"> (PIV or common access card (CAC)) and derived credentials Cert MFA Password Establish or manage attributes <ul style="list-style-type: none"> Organization Groups/Roles Manage or 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) (05-15-2025)

Logging Requirements – Technical Details

Log Category	Required Data	Format	Criticality	Retention Period
Privileged Identity & Credential Management	Privileged Identity & Credential Management <ul style="list-style-type: none"> Provisioning Manage credential type <ul style="list-style-type: none"> (PIV or CAC) and derived credentials Cert MFA Password Establish or manage attributes <ul style="list-style-type: none"> Organization Groups/Roles Manage or 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 <ul style="list-style-type: none"> Commands Tasks Track privilege escalation and delegation Monitor, alert and respond to anomalous behaviors or 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 <ul style="list-style-type: none"> DHCP lease information Including: <ul style="list-style-type: none"> MAC IP 	Log	0	12 months active storage 18 months cold data storage

Exhibit 10.8.63-5 (Cont. 3) (05-15-2025)**Logging Requirements – Technical Details**

Log Category	Required Data	Format	Criticality	Retention Period
Network Device Infrastructure	DNS - Source IP and Port, Destination IP and Port Date and Time <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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

Exhibit 10.8.63-5 (Cont. 4) (05-15-2025)

Logging Requirements – Technical Details

Log Category	Required Data	Format	Criticality	Retention Period
Network Device Infrastructure	DNS, DHCP, and Wi-Fi <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Static network address translation table mapping as well as port forwards <ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)/Network Traffic Analysis (NTA)/Network Detection and Response (NDR)/SIEM Logs Application programming interface (API) activity logs Authentication logs Firewall logs Web proxy/web application firewall (WAF) logs Service metrics Network flow logs Remote access/VPN logs System/operating 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

Exhibit 10.8.63-5 (Cont. 5) (05-15-2025)**Logging Requirements – Technical Details**

Log Category	Required Data	Format	Criticality	Retention Period
Network Device Infrastructure (For Devices with Multiple Interfaces: Interface MAC -If Correlated to The De-NAT IP Address)	Routers and Switches <ul style="list-style-type: none"> • Routing tables • Routing changes (logging all CLI commands, border gateway protocol (BGP)) • IP addressing schema and implementation 	Log File Config	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)	Load Balancer/Reverse Proxy Access Logs <ul style="list-style-type: none"> • 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 • Secure sockets layer (SSL) cipher • SSL protocol • Server name indication (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

Exhibit 10.8.63-5 (Cont. 6) (05-15-2025)**Logging Requirements – Technical Details**

Log Category	Required Data	Format	Criticality	Retention Period
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, World Wide Web Consortium (W3C) Format. <ul style="list-style-type: none"> • Date and time • Source <ul style="list-style-type: none"> • Hostname • IP address and port • MAC • Destination <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Policy updates • Software updates 	Log	0	12 months active storage 18 months cold data storage

Exhibit 10.8.63-5 (Cont. 7) (05-15-2025)**Logging Requirements – Technical Details**

Log Category	Required Data	Format	Criticality	Retention Period
Proxies and Web Content Filters • Policy Updates • Software Updates	General Information <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Startup and shutdown of the system • Startup and shutdown of a service • Network connection changes or failures • Changes to, or attempts to change, system security settings and controls OS Audit Records <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Application authentication attempts (success/failure) • Application account changes (e.g., account creation and deletion, account privilege assignment) • Use of application privileges 	Log	0	12 months active storage 18 months cold data storage

Exhibit 10.8.63-5 (Cont. 8) (05-15-2025)

Logging Requirements – Technical Details

Log Category	Required Data	Format	Criticality	Retention Period
	Application Operations <ul style="list-style-type: none">• Application startup and shutdown• Application failures• Major application configuration changes• Application transactions, for example,<ul style="list-style-type: none">• 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) (05-15-2025)**Logging Requirements – Technical Details**

Log Category	Required Data	Format	Criticality	Retention Period
Operating Systems Windows Infra-structure and Operating Systems	<p>User and Administrator Access to OS Components and Applications</p> <ul style="list-style-type: none"> • File and object access • Audit log access (success/failure) • System access and log off (success/failure) • Privilege access and log off (success/failure) • Remote desk protocol (RDP) access and log off (success/failure) • Server message block (SMB) access • Installation or removal of storage volumes or removable media <p>System Performance and Operational Characteristics</p> <ul style="list-style-type: none"> • Resource utilization, process status • System events • Service status changes (start, stop, fail, restart, etc.) • Service failures and restarts • Process creation and termination <p>System Configuration</p> <ul style="list-style-type: none"> • Changes to security configuration (success/failure) • Audit log cleared • Changes to accounts • User or group management changes • Scheduled task changes <p>File Access</p> <ul style="list-style-type: none"> • Transfer of data to external media or remote hosts <p>Host Network Communications</p> <ul style="list-style-type: none"> • Listening network port and IP address • Active network communication with other hosts 	Log	0	<p>12 months active storage</p> <p>18 months cold data storage</p>

Exhibit 10.8.63-5 (Cont. 10) (05-15-2025)

Logging Requirements – Technical Details

Log Category	Required Data	Format	Criticality	Retention Period
	Powershell Execution Commands WMI Events Registry Access Command-Line Interface (CLI) Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware <ul style="list-style-type: none">• Version• Created date• Installed date• Manufacturer			

Exhibit 10.8.63-5 (Cont. 11) (05-15-2025)

Logging Requirements – Technical Details

Log Category	Required Data	Format	Criticality	Retention Period
Operating Systems MACOS (Or Other Apple Desktop and Server Operating Systems)	<p>User and Administrator Access to OS Components and Applications</p> <ul style="list-style-type: none"> • File and object access • Auditlog 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/Network File System (NFS)/(S)File Transfer Protocol (FTP) or equivalent access • Installation or removal of applications • Installation or removal of storage volumes or removable media <p>System Performance and Operational Characteristics</p> <ul style="list-style-type: none"> • Resource utilization, process status • System events • Service status changes (start, stop, fail, restart, etc.) • Service failures and restarts • Process creation and termination <p>System Configuration</p> <ul style="list-style-type: none"> • Changes to security configuration (success/failure) • Audit log cleared • Changes to accounts • User or group management changes • Scheduled task changes <p>File Access</p> <ul style="list-style-type: none"> • Transfer of data to external media or remote hosts <p>Host Network Communications</p> <ul style="list-style-type: none"> • Listening network port and IP address • Active network communication with other hosts 	Log	0	<p>12 months active storage</p> <p>18 months cold data storage</p>

Exhibit 10.8.63-5 (Cont. 12) (05-15-2025)

Logging Requirements – Technical Details

Log Category	Required Data	Format	Criticality	Retention Period
	Command-Line Interface (CLI) <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Version Created date Installed date Manufacturer 			

Exhibit 10.8.63-5 (Cont. 13) (05-15-2025)

Logging Requirements – Technical Details

Log Category	Required Data	Format	Criticality	Retention Period
Operating Systems – BSD (Linux)	<p>User and Administrator Access to OS Components and Applications</p> <ul style="list-style-type: none"> • 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 removable media <p>System Performance and Operational Characteristics</p> <ul style="list-style-type: none"> • Resource utilization, process status • System events • Service status changes (start, stop, fail, restart, etc.) • Service failures and restarts • Process creation and termination <p>System Configuration</p> <ul style="list-style-type: none"> • Changes to security configuration (success/failure) • Audit log cleared • Changes to accounts • User or group management changes • Scheduled task changes <p>File Access</p> <ul style="list-style-type: none"> • Transfer of data to external media or remote hosts <p>Host Network Communications</p> <ul style="list-style-type: none"> • Listening network port and IP address • Active network communication with other hosts 	Log	0	<p>12 months active storage</p> <p>18 months cold data storage</p>

Exhibit 10.8.63-5 (Cont. 14) (05-15-2025)

Logging Requirements – Technical Details

Log Category	Required Data	Format	Criticality	Retention Period
	Command-Line Interface (CLI) Security Enhanced Linux (SELinux) AppArmor or Equivalent <ul style="list-style-type: none"> Warning logs Violation logs System <ul style="list-style-type: none"> /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 <ul style="list-style-type: none"> /Var/Log/Auth.Log /Var/Log/Secure /Var/Log/Faillog /Var/Log/Btmp /Var/Log/Wtmp or /Var/Log/Utmp Applications <ul style="list-style-type: none"> /Var/Log/Mail.Log or /Var/Log/Maillog /Var/Log/Xorg.X.Log Package Install/Uninstall <ul style="list-style-type: none"> /Var/Log/Dpkg.Log /Var/Log/Yum.Log Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware <ul style="list-style-type: none"> Version Created date Installed date Manufacturer 			

Exhibit 10.8.63-5 (Cont. 15) (05-15-2025)**Logging Requirements – Technical Details**

Log Category	Required Data	Format	Criticality	Retention Period
Cloud Environments (General Events)	<p>Nearly all successful attacks on cloud services result from customer misconfigurations. With that in mind, the logging and monitoring focus should be on:</p> <ul style="list-style-type: none"> 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	<p>12 months active storage</p> <p>18 months cold data storage</p>
Cloud Environments (General Logging)	<ul style="list-style-type: none"> 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	<p>12 months active storage</p> <p>18 months cold data storage</p>

Exhibit 10.8.63-5 (Cont. 16) (05-15-2025)

Logging Requirements – Technical Details

Log Category	Required Data	Format	Criticality	Retention Period
Cloud AWS	<ul style="list-style-type: none"> • AWS CloudTrail • Amazon CloudWatch logs • AWS Config • Amazon S3 access logs • Amazon virtual private cloud (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	<ul style="list-style-type: none"> • Azure active directory logs • Activity logs • Unified audit logs (with advanced audit features) 	Log	0	12 months active storage 18 months cold data storage
Cloud GCP	<ul style="list-style-type: none"> • Access transparency audit log • Adminaudit 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: <ul style="list-style-type: none"> • 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. 17) (05-15-2025)**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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Authentication logons (success/failure) Authentication logoffs Privilege elevation (success/failure) Security related system alerts and failures User and group <ul style="list-style-type: none"> 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. 18) (05-15-2025)**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: <ul style="list-style-type: none"> • “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	<ul style="list-style-type: none"> • Date and time source hostname <ul style="list-style-type: none"> • IP • Port • Destination hostname <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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. 19) (05-15-2025)**Logging Requirements – Technical Details**

Network Device Infrastructure	All Devices <ul style="list-style-type: none"> • Hash of the binary / binaries running on the device • Hash of configs • Firmware <ul style="list-style-type: none"> • 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 (ACLs) are enabled and the device is filtering traffic: <ul style="list-style-type: none"> • Action permit, teardowns, closes, denies, and drops • Interface • Source <ul style="list-style-type: none"> • Hostname • IP address and port • MAC • Destination <ul style="list-style-type: none"> • Hostname • IP address and port • MAC • Protocol type • Rule name and number triggers • 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. 20) (05-15-2025)**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 <ul style="list-style-type: none"> • Date and time • Source <ul style="list-style-type: none"> • Hostname • IP address and port • MAC • Destination <ul style="list-style-type: none"> • Hostname • IP address and port • MAC • Signature triggered and associated details including: <ul style="list-style-type: none"> • 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. 21) (05-15-2025)**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: <ul style="list-style-type: none"> • Date and time • Source <ul style="list-style-type: none"> • Hostname • IP address and port • MAC • Destination <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. 22) (05-15-2025)

Logging Requirements – Technical Details

Vulnerability Assessments	<ul style="list-style-type: none">• 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. 23) (05-15-2025)**Logging Requirements – Technical Details**

Database Level	<ul style="list-style-type: none"> • Addition of new users, especially privileged users • Query being executed • Query, status (response), and traceback <ul style="list-style-type: none"> • 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 database • 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. 24) (05-15-2025)**Logging Requirements – Technical Details**

Application Level	Web Applications <ul style="list-style-type: none"> • URL • Headers • HTTP methods - Request with body of data <ul style="list-style-type: none"> • This data must be evaluated to ensure proper protections are in place to encrypt the data at rest and in transit. Tools must be accredited to handle sensitive data and proper oversight controls must be implemented to look for signs of inappropriate data usage. • HTTP response with body of data 	Log Log and packet capture (PCAP) of plaintext HTTP request and response with data	1	12 months active storage 18 months cold data storage
Application Level	Web Applications <ul style="list-style-type: none"> • Database queries • Response codes 	Log	1	12 months active storage 18 months cold data storage
Application Level	Web Applications Crashes <ul style="list-style-type: none"> • Processes • Applications 	Log	1	12 months active storage 18 months cold data storage
Application Level	Web Applications & Middleware <ul style="list-style-type: none"> • Configuration • Version 	Log	1	12 months active storage 18 months cold data storage

Exhibit 10.8.63-5 (Cont. 25) (05-15-2025)**Logging Requirements – Technical Details**

Virtualization System	<ul style="list-style-type: none"> • User authentication <ul style="list-style-type: none"> • Logon (success and failure) • Attempts to obtain privileged access (success and failure) • User and administrator/root access and actions of components and applications <ul style="list-style-type: none"> • File and object access • Audit log access (success and failure) • System access (failure) • System performance and operational characteristics <ul style="list-style-type: none"> • Resource utilization, process status • System events • Service status changes (e.g., started, stopped) • System configuration <ul style="list-style-type: none"> • Changes to security configuration (success/failure) • Changes to hypervisor • Changes to vulnerability management service (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. 26) (05-15-2025)**Logging Requirements – Technical Details**

Mobile (Smart-phones and Tablets) EMM (UEM) / MTD Server Logs	EMM (UEM)/Mobile Threat Defense (MTD) Alerts <ul style="list-style-type: none">• Date and time• Alert type• Failure of cryptographic protocols• Failure of device cryptographic capabilities (e.g., trusted boot process)• Certificate validation failure (defined in mobile device management (MDM) server protection 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. 27) (05-15-2025)**Logging Requirements – Technical Details**

Mobile (Smart-phones and Tablets) EMM (UEM) / MTD Agent Logs	<p>General:</p> <ul style="list-style-type: none"> • Date and time <p>Device Data</p> <ul style="list-style-type: none"> • Device name • Device manufacturer and model • Serial # • Phone # • International mobile equipment identity (IMEI), international mobile subscriber identity (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 <p>Application Data</p> <ul style="list-style-type: none"> • Application manifest (installed apps, app version, version history and installation time-stamps), installation and data storage location • Application permissions • Application hash (e.g., SHA256) • Running apps and processes <p>Device Policy Settings</p> <ul style="list-style-type: none"> • Enrollment policies • Policies successfully/ unsuccessfully applied • Authentication policies (password/PIN/biometric, etc.) <p>Device Configuration</p> <ul style="list-style-type: none"> • Certificates end related information (validity period, revocation, etc.) • Device encryption configuration • Android enterprise settings • System integrity status 	Log	1	<p>12 months active storage</p> <p>18 months cold data storage</p>
--	--	-----	---	--

Exhibit 10.8.63-5 (Cont. 28) (05-15-2025)**Logging Requirements – Technical Details**

	<p>Network Configuration</p> <ul style="list-style-type: none"> • 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 MACaddress • Bluetooth <p>Event/Audit/Crash Logs</p> <ul style="list-style-type: none"> • Event type and ID • Event date/timestamp • Success or failure of various services • User authentication (success or failure) • Event actor and ID (e.g., admin, system, device) • Event change type (create, read, update, and delete (CRUD)) <p>MTD Agent Info</p> <ul style="list-style-type: none"> • Agent activation status • Threat detection of a variety of vulnerabilities • Phishing protection status • Tampering of agent, app, or system • Privilege escalation • Man in the middle (MITM) activities • Remediation actions taken • Last time device synched with enterprise 			
Container - Supply Chain	<ul style="list-style-type: none"> • 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	<p>12 months active storage</p> <p>18 months cold data storage</p>

c. Criticality = 2

Exhibit 10.8.63-5 (Cont. 29) (05-15-2025)**Logging Requirements – Technical Details**

Log Category	Required Data	Format	Criticality	Retention Period
System Configuration and Performance	System Status <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Date and time Sent from sender Recipient Subject Email headers Rule Triggered – Log of policies along with actual values including but not limited to: <ul style="list-style-type: none"> DNS records Phish campaign identifier Domain URL <p>Note: Federal agencies must submit all phishing attempts to CISA by forwarding the phishing as an attachment to <i>federal.phishing.report@us-cert.gov</i>. Federal agencies must ensure that all contractors that operate infrastructure on their behalf implement this requirement.</p>	Log Email attachments	2	12 months active storage 18 months cold data storage
Data Loss Prevention	<ul style="list-style-type: none"> Date and time Source hostname <ul style="list-style-type: none"> IP Port Destination Hostname <ul style="list-style-type: none"> 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. 30) (05-15-2025)**Logging Requirements – Technical Details**

Network Traffic	Full Packet Capture Data <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> User authentication (success/failure) User and administrator application use: <ul style="list-style-type: none"> File and object access Audit log access (success/failure) System access (failure) Application transactions (web page this, email sent/received, file transfers completed) Transaction logs System performance and operational characteristics <ul style="list-style-type: none"> 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. 31) (05-15-2025)**Logging Requirements – Technical Details**

Application Level	General – Non-COTS <ul style="list-style-type: none"> • User authentication (success/failure) • User access of application components <ul style="list-style-type: none"> • File and object access • Audit log access (success/failure) • System access (failure) • Application transactions • Transaction logs • System performance and operational characteristics <ul style="list-style-type: none"> • 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. 32) (05-15-2025)**Logging Requirements – Technical Details**

Container - Image	<ul style="list-style-type: none"> • 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) • 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)	<ul style="list-style-type: none"> • 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. 33) (05-15-2025)**Logging Requirements – Technical Details**

Container - OS	<ul style="list-style-type: none"> User and administrator access to OS components and applications <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Resource utilization process status System events Service status changes (start, stop, fail, restart) Service failures and restarts Process creation and termination System configuration <ul style="list-style-type: none"> Changes to security configuration (success/failure) Audit log cleared Changes to accounts user or group management changes Scheduled task changes File access <ul style="list-style-type: none"> 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. 34) (05-15-2025)**Logging Requirements – Technical Details**

System Configuration and Performance	Software Updates <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Syslog & Syslogd data Log4j data Sysout data resource measurement facility (RMF) data System management facility (SMF) <p>Note: See DISA's zOS Mainframe STIG for log configuration guidance</p> <ul style="list-style-type: none"> Output from integrated intrusion detection services 	Log	3	12 months active storage 18 months cold data storage
Container -Cluster/ Pod Events	<ul style="list-style-type: none"> 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

