MANUAL TRANSMITTAL

10.8.33

Department of the Treasury
Internal Revenue Service

NOVEMBER 3, 2023

EFFECTIVE DATE

(11-03-2023)

PURPOSE

(1) This transmits revised Internal Revenue Manual (IRM) 10.8.33, *Information Technology (IT) Security, Mainframe System Security Policy.*

MATERIAL CHANGES

(1) IRM 10.8.33.1, Program Scope and Objectives - Updated section to align with Security Policy Boiler Plate.

(2) IRM 10.8.33.1.1.1 Scope was removed.

(3) IRM 10.8.33.1.1.2 Objectives was removed.

(4) IRM 10.8.33.1.4 Program Management and Review updated with language from IRM 10.8.33.1.1.1.

(5) IRM 10.8.33.2 Roles and Responsibilities moved to a new subsection IRM 10.8.33.3.

(6) Exhibit 10.8.33-1 Security Requirements Checklists was updated with language from IRM 10.8.33.1.1.1 Scope.

(7) IRM 10.8.33-2, Glossary and Acronyms - is now Terms and Acronyms to align with SPDER and updated with grammatical edits and corrections.

(8) IRM 10.8.33-3, References - is now Related Resources

EFFECT ON OTHER DOCUMENTS

IRM 10.8.33 dated March 1, 2023, is superseded. This IRM supersedes all prior versions of IRM 10.8.33. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* and IRM 10.8.2, *Information Technology (IT), IT Security Roles and Responsibilities*.

AUDIENCE

IRM 10.8.33 shall be distributed to all personnel responsible for overseeing, managing, and implementing IRS mainframe information and information systems. This policy applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya
Acting, Chief Information Officer

10.8.33
Mainframe System Security Policy

Table of Contents

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

#
#
#
#
#
#

Exhibits

10.8.33.1
(11-03-2023)
Program Scope and Objectives

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

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

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

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

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

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

(5) **Program Owner:** Cybersecurity Threat Response & Remediation (an organization within Cybersecurity).

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

10.8.33.1.1
(02-24-2022)
Background

(1) This IRM defines the security controls for the protection of IRS mainframe systems.

(2) FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, mandates the use of NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* , as an initial set of baseline security controls for the creation of agency IT security policy.

(3) IRM 10.8.33 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

(4) This IRM replaces the following IRMs:

a. IRM 10.8.30, *Information Technology (IT) Security, Unisys Operating System (OS) Security Standards*.
b. IRM 10.8.32, *Information Technology (IT) Security, IBM Mainframe System Security Requirements*.

Note: Security guidance specific to the platforms in the replaced IRMs have been incorporated into this IRM. Additionally, the Security Checklists for the replaced IRMs have been incorporated into this IRM.

10.8.33.1.2
(03-01-2023)
Authority

(1) IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, establishes the security program and the policy framework for the IRS.

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

10.8.33.1.3
(11-03-2023)
Roles and Responsibilities

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

(2) The supplemental roles and responsibilities provided below are specific to the implementation of IBM Mainframe Product Systems.

Note: No specific roles are listed within this IRM for Unisys.

(3) For the purpose of this IRM, the table below is a correlation between the IBM Mainframe Product Roles referred to within the Vanguard Configuration Manager (VCM) to a corresponding IRS Role defined either within this IRM or IRM 10.8.2.

Note: These VCM roles are defined in the DISA STIGs.

IBM Mainframe Product Role	IRS Role
Systems Programmer	System Administrator (SA)
Security Administrator	Resource Access Control Facility (RACF) System Administrator (RSA)
Information System Security Manager (ISSM)	Information System Security Officer (ISSO)
Information Assurance Officer (IAO)	ISSO
Auditor	Security Specialist (SecSpec)
	ISSO
Audit Personnel	SecSpec
	ISSO
	RACF System Auditor
	RACF Group Auditor

(4) Refer to IRM 10.8.2 for additional information regarding organizational and individual responsibilities related to information and computer security.

10.8.33.1.3.1
(11-03-2023)
System Programmer

(1) A System Programmer in the z/OS Support Section is responsible for installing and updating the RACF security product on the IBM Mainframes as part of regularly scheduled z/OS upgrades and/or maintenance.

10.8.33.1.3.2
(11-03-2023)
Resource Access Control Facility (RACF) System Administrator (RSA)

(1) A RACF System Administrator (RSA) is in the System Administrator role, with a subset of the generic system administrator responsibilities.

(2) The RSA maintains the security product and shall:

a. Identify and maintain security system level resources.
b. Perform the initial setup of the RACF system.
c. Have overall responsibility for all security matters within RACF.

(3) The RSA, in coordination with the operating system program developer(s), systems operations staff, shall identify and install all critical system resources, components, data sets, and connections which are to be protected by RACF. The RSA shall:

a. Implement the RACF setup for System Datasets, Resources Profiles, and Data Sets associated with those Resources, and is responsible for information as to its setup.
b. Determine the owner(s) of the aforementioned resources.

(4) The RSA determines the appropriate access control levels and monitoring requirements for system resources by:

a. Configuring system parameters within the documented security standards, using the applicable IRMs and system life cycle documentation.
b. Maintaining current documentation that properly defines the technical hardware and software configuration of system and network connections.
c. Starting up and shutting down the system.
d. Ensuring regular backups, recovery tests, and other associated contingency planning responsibilities for systems are performed.

Note: This responsibility is conducted in an oversight capacity.

e. Monitoring system/user access for performance concerns.
f. Performance application management activities.

(5) The RACF System Administrator shall participate in contingency planning and contingency plan testing activities, as specified by IRM 10.8.1, IRM 10.8.60, *IT Service Continuity Management (ITSCM) Policy and Guidance,* and IRM 10.8.62, *Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Program.*

10.8.33.1.3.3
(11-03-2023)
Resource Access Control Facility (RACF) User and Group Administrator

(1) The RACF User Administrator (RUA) performs user account administration in collaboration with the RACF System Administrator (RSA). The RUA shall:

a. Perform the initial setup of user and group access profiles.
b. Establish and maintain least privilege user roles and the role based access matrix outlining the access for each role.
c. Ensure that users are established using an access control system (e.g., Business Entitlement Access Request System (BEARS) or once required approvals are satisfied.
d. Perform application management activities.

(2) The RACF Group Administrator functions within the Security Administrator role and performs user account administration at the group level. Distributed security administration is allowed, but not required.

a. RACF Group Administrators shall have overall responsibility for all security matters within the scope of their group.

10.8.33.1.3.4
(11-03-2023)
Resource Access Control Facility (RACF) System and Group Auditor

(1) The RACF System or Group Auditor, functions within the Security Specialist role. Refer to the Security Specialist (SecSpec) section within IRM 10.8.2 for general requirements.

a. Independent auditor(s) are assigned at the system or user group level; to provide a system of checks and balances; and
b. Independent auditor(s) shall review user activities in areas where they perform no activities relating to administration, programming, or security administration.

10.8.33.1.4
(11-03-2023)
Program Management and Review

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

(2) It is the policy of the IRS:

a. To establish and manage an Information Security Program within all its offices. This policy provides uniform policies and guidance to be used by each office.
b. To 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. To protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, Office of Management and Budget (OMB) guidance, the Department of the Treasury Directives (TDs), NIST Publications, National Archives and Records Administration (NARA) guidance, other regulatory guidance, and best practice methodologies.
d. To use best practices methodologies (such as Capability Maturity Model Integration (CMMI), Enterprise Life Cycle (ELC), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.33.1.5
(11-03-2023)
Program Controls

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

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

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

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

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

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

10.8.33.1.6
(11-03-2023)
Terms and Acronyms

(1) Refer to Exhibit 10.8.33-2 for a list of terms, acronyms, and definitions.

10.8.33.1.7
(11-03-2023)
Related Resources

(1) Refer to Exhibit 10.8.33-3 for a list of related resources and references.

10.8.33.1.8
(03-01-2023)
Risk Acceptance and Risk-Based Decisions

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

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

a.
b. Use Online RBD, as described in the Request for Risk Acceptance Request and Risk-Based Decision (RBD) Standard Operating Procedures (SOP), available in the Security Risk Management (SRM) FISMA Document Library, on the Enterprise FISMA Compliance SharePoint site via the Risk Acceptance Requests link at: *https://irsgov.sharepoint.com/sites/CyberSRM/SitePages/RiskBasedDecision.aspx.* Website.

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

#
#
#
#
#

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

#
#

#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#

#
#

#
#

#
#

#
#

#
#

#
#

#
#
#
#
#
#

#
#

#
#

#
#
#
#
#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#
#
#

#
#

#

#
#
#
#
#

#
#

#
#
#

#
#
#

#
#

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

#

#
#
#
#
#
#

#

#

#

#

#

#
#
#
#

#

#

#

#

#

#

#

#

#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#

#
#

#
#

#
#
#

#
#

#
#

#
#
#

#
#

#
#

#
#
#

#
#

#
#

#
#
#

#
#

#
#

#
#
#

#
#

#
#

#
#

#

#
#
#
#

#
#

#
#

#
#

#
#
#
#
#
#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#

#

#

#

#
#
#
#
#

#

#
#
#
#
#

#
#
#

#
#

#
#
#

#
#

#
#
#

#
#

#

#
#

#
#

#
#
#
#

#
#
#
#
#

#

#

#
#
#
#
#

#
#

#
#
#
#
#
#
#
#
#
#

#

#
#
#
#

#
#

#

#
#

#
#

#
#

#
#

#
#

#
#
#

#
#

#
#

#
#

#

#
#

#
#

#
#
#
#
#

#
#
#

#
#

#

#
#
#

#
#
#

#

#
#
#
#

#
#
#
#

Exhibit 10.8.33-1 (03-01-2023)
Security Requirements Checklists

1. Security Requirements Checklists (if accompanying this IRM) serve as the secure configuration baseline and are developed in accordance with NIST Special Publication (SP) 800-70, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers:

a. IRMs with accompanying checklists contain a checklist with general security requirements (e.g., Defense Information Systems Agency (DISA), Security Requirements Guide (SRG)), as well as checklists with platform or technology specific security requirements (e.g., Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) Benchmarks). In the event a platform or technology specific security checklist is not available, the general security requirements checklist shall be used (e.g., Database (General), Operating System (General), Router (General)).
b. Security Requirements Checklists shall be used in addition to the IRS and the Department of the Treasury defined requirements within the IRM.
c. In the event of a conflict between a checklist and this IRM, excluding the Department of the Treasury defined requirements, the requirement(s) from the checklist shall take precedence.

Note: The order of precedence only applies when there is a conflict between the IRM and one of its accompanying checklists and does not apply when there is a discrepancy with IRM 10.8.1.

d. The order of precedence only applies when there is a conflict between the IRM and one of its accompanying checklists and does not apply when there is a discrepancy with IRM 10.8.1.

2. The technical security requirements for mainframe systems are maintained in one or more Excel security checklists (spreadsheets). Per IRM 10.8.1 Baseline Configuration (CM-2) and Configuration Settings (CM-6) guidance, IRS security checklists are derived from DISA security guides (SRGs, STIGs, etc.), CIS benchmarks, and/or vendor provided guides and shall be used on all IRS systems. These checklists are available within the "Security Requirements Checklists" folder on the IRS Cybersecurity Security Policy SharePoint site at:

#

a. a) Select the appropriate IRM folder.
b. Security Requirements Checklists are available for the following:

- Mainframe Product – General Baseline
- Management Consoles
- Unisys
- zOS RACF
- zVM

3. Security Checklists shall be effective immediately. Vulnerabilities shall be remediated in accordance with IRM 10.8.50 Information Technology (IT) Security, Servicewide Security Patch Management, remediation timelines table. The source's publication date can be found in the external reference row of the checklist. (Typically row 10)

4. Checklists for technologies identified as Beyond Sunset or Removed by Enterprise Architecture (EA) Enterprise Standards Profile (ESP) will not receive further updates. These checklists will be removed from the active checklist and moved to an Archive folder during the next checklist update cycle.

5. Evaluate system configurations and implement controls while protecting system functionality.

Exhibit 10.8.33-2 (02-24-2022)
Terms and Acronyms

Terms and Acronyms	
Access control	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).
ACR	Access Control Record - A record containing a list of users, the accesses they may have to an object and the conditions under which they are allowed access.
Access List	A discretionary control owners give to an object. Access lists are public, private, or semiprivate.
Access Matrix	A grid form matrix which shows the dataset profile names and the access level of the groups
Account Name	An identifier specifying an account charged with processing time and system resources consumed during a run. Account names can be used to control access to objects by specifying them in ACRs.
ACIO	Associate Chief Information Officer
ACP	Access Control Products
ADS	Application Development System
AES	Advanced Encryption Standard
Alpha characters	Characters, generally in a password, that represent only the letters, A through Z.
Alphanumeric characters	Characters, generally in a password, that represents letters, A through Z, and numbers, 0 through 9.
AO	Authorizing Official
APF	Authorized Program Facility
Attributes	A security characteristic of a subject or object. When compared between subjects and objects, attributes determine which objects and what types of access subjects are authorized to access. Attributes include both mandatory and discretionary controls: project-id, account name, clearance level and clearance level range, security record owner, trusted privilege set, access list, and read-only/write-only.
Audit	An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.
Authorization	The access right granted to a user allowing communication with a computer system to access an object, resource, or function.
Backup Procedures	The provisions made in a contingency plan for the recovery of data and for restart or replacement of computer equipment after a system failure or disaster.

Exhibit 10.8.33-2 (Cont. 1) (02-24-2022)
Terms and Acronyms

Batch Run	A set of instructions a user submits as a complete job. Batch runs are designed to execute independently from start to finish and requires no further instructions or parameters.
BEARS	Business Entitlement Access Request System
C2	A level of security designated by NIST which authentication of users on the system. Its base requirement is that users and applications need to be authenticated before they are allowed to use a resource administered by the operating system.
CA	Certificate Authority
CICS (Customer Information Control System)	A general purpose program that controls on–site communication between terminal users and a database.
CM	Configuration management
CMP	Change Management Process
CNF	Certified Name Filters
Common Criteria	An international standard for information technology security evaluation. Replaces Department of Defense orange book and others in the rainbow series (i.e., C2 level of security).
COTS	Commercial Off the Shelf
CPE	Computer Performance Engineer
CRL	Certificate Revocation List
CSA	Computer Systems Analyst
CSIRC	Computer Security Incident Response Center
DAC	Discretionary Access Control - An access control policy that is enforced over all subjects and objects in an information system where the policy specifies that a subject that has been granted access to information can do one or more of the following: (i) pass the information to other subjects or objects; (ii) grant its privileges to other subjects; (iii) change security attributes on subjects, objects, information systems, or system components; (iv) choose the security attributes to be associated with newly-created or revised objects; or (v) change the rules governing access control. Mandatory access controls restrict this capability.
DBA	Database Administrator
DASD	Direct Access Storage Device
Data Security Monitor	An auditing tool that produces reports which enables a security administrator to verify basic system integrity and controls
DBMS	Database Management System

Exhibit 10.8.33-2 (Cont. 2) (02-24-2022)
Terms and Acronyms

DES	Data Encryption Standard -. In computer security, NIST, Data Encryption Standard, adopted by the U.S. government in FIPS Publication 46, which allows only hardware implementations of the data encryption algorithm. The algorithm is 64 bit block cipher that uses a 64 bit key, of which 56 bits are used to control the cryptographic process and 8 bits are used for parity checking to ensure that the key is transmitted properly.
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DFSMS	Data Facility Storage Management Subsystem
DR	Disaster Recovery
DSA	Data Storage Analyst
EA	Enterprise Architecture
EO	Executive Order
ELC	Enterprise Life Cycle
ER	Executive Request - An instruction that causes the Exec to perform a service function. Selected ERs affect system security. The ability to execute these ERs is controlled, which allows specified users to override security restrictions and validations
ESM	External Security Manager – An application outside the operating system that provides a layer of security to various system artifacts.
ESP	Enterprise Standards Profile
File	An organized collection of data, treated as a unit, and stored so as to facilitate the retrieval of each individual data item.
FIRECALL UserID	A privileged user-id used only in emergency situations when privileged users are not available.
FIPS	Federal Information Processing Standards
FISMA	The E-Government Act of 2002 (P.L. 107-347) Title III, Federal Information Security Modernization Act of 2014
FIT	Final Integration Test
Foreign UserIDs	A term that was created at the 1999 IRS Security Conference to identify those UserIDs associated with FTP processing. These Ids may be associated with Tier II systems
Form 5389	Separating Employee Clearance Certificate
FTP	File Transfer Protocol
FY	Fiscal Year

#
#

Exhibit 10.8.33-2 (Cont. 3) (02-24-2022)
Terms and Acronyms

GAO	Government Accountability Office - The organization that monitors government agencies to ascertain compliance with the appropriate laws and standards (e.g., DHS, NIST, OMB).
Group	A collection of users who can share access authorities for protected resources.
HFS	Hierarchical File System
IBM	International Business Machines
Independent Auditor	See Independent Assessor or Assessment Team
Independent Assessor or Assessment Team	Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. (NIST SP 800-53)
Information Systems	An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, and control data or information. An information system shall typically consist of automated data processing system hardware, operating system and application software, associated peripheral devices, and associated data communications equipment.
I/O	Input/Output
IPF	Interactive Processing Facility
IPL	Initial Program Load
IRM	Internal Revenue Manual
IS	Information Systems
ISCP	Information Systems Contingency Plan
ITSCM	IT Service Continuity Management
ISSO	Information System Security Officer
IT	Information Technology
ITAMS	Information Technology Asset Management System
LDAP	Lightweight Directory Access Protocol

Exhibit 10.8.33-2 (Cont. 4) (02-24-2022)
Terms and Acronyms

Least Privilege	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
LEM	Law Enforcement Manual
LPAR	Logical Partition
MAC	Mandatory Access Control - An access policy that restricts access to system objects (e.g., files directories, devices) based on the sensitivity of the information in the object (represented by the objects label) and the authorization of the subject (usually represented by the user's clearance) to access information at that sensitivity level. Mandatory means that the system enforces the policy; users do not have the discretion to share their files. Contrast with Discretionary Access Control (DAC).
		#
MCS	Multiple Console Support
MFD	Master File Directory
		#
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSO	Network Security Officer
Numeric characters	Any one of the digits 0 (zero) through 9.
NVB	National Vulnerability Database
Object	An entity containing information that resides on the computer system. Objects include files, tape volumes, and subsystems
Object Reuse	The assurance that a storage object (e.g., disk, magnetic media) is initially assigned, allocated, or reallocated to a system user who has been cleared.
ODB	Operations Data Base
OMB	Office of Management and Budget
OS	Operating System
Ownership	An operating system feature that assigns owners to objects. With ownership, users own every object they create and determine whether they want to give access to other users.
Password	A string of characters known to the computer system and a user, who must specify it to gain full or limited access to a system and to the data stored therein.
PC	Program Call

Exhibit 10.8.33-2 (Cont. 5) (02-24-2022)
Terms and Acronyms

PIV	Personal Identity Verification
Privilege	The mechanism that allows specified users to perform security relevant actions within the operating system. In the case of trusted privileges, the mechanism that allows specified users to override MAC and DAC controls.
PROD	Production System
RBD (Risk Based Decision Process)	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).
RIS	Request for Information Services
SA	System Administrator
SAT	System Application Testing
SA&A	Security Assessment and Authorization
SBU	Sensitive But Unclassified - Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals a entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.
SCDC	Source Code and Documentation Control
SDSF	System Display and Search Facility
SEID	Standard Employee Identification Code
SEO	Office of Security Policy Support and Evaluation
Security	The protection of resources from damage or misuse and the protection of data against accidental or intentional disclosure to unauthorized persons or unauthorized modifications or destruction.
Security Analyst	An individual who administers security on a given computer platform.
Security Policy	The set of rules and practices that regulate how an organization manages, protects, and distributes sensitive information.
Secured Executive Requests	A set of ERs that only designated users can use. Semiprivate - A private object to which the owner has access but to which other subjects have access only as specified by an attached access control record (ACR). The ACR provides a discretionary access list mechanism for the owner of the private object.

Exhibit 10.8.33-2 (Cont. 6) (02-24-2022)
Terms and Acronyms

Service Centers	Originally 10 centers that did the computer work for the tax returns. As each has been consolidated into a Computing Center, it was no longer considered a Service Center but a Campus (e.g., Kansas City Campus).
SIMAN	The Site Management Complex - A program that security officers, system administrators, and users use to install and update records in the security and resource control databases
SMF	System Management Facility
SMP/E	System Modification Program/Extended
SMS	System Management Services
SOP	Standard Operating Procedure
SPO	Single Point Operations Console
SPI	System Programming Interfaces
SQuA	Software Quality Assurance - A Commercial Off the Shelf (COTS) product from Arkdata that is tailored to the IRS environment and resides on the Development System to provide version control, standardized compilation process, and a mechanism for SCDC to control the transmittal of software/scripts to the SAT/FIT system and the Production Transmittal Software.
SRM	Security Risk Management
SSD	System Support Division
SSL	Secure Sockets Layer
SSG	Symbolic Stream Generator
SSP	System Security Plan
SUA	Standard Unit of Accounting
Subsystem	A software entity, with an addressing environment and a set of security attributes that protect the rest of the system by a combination of hardware and software mechanisms that control access. The main types of subsystem are: protected (both object module and common bank) and chameleon/library common bank. A protected subsystem is typically a subject acting on behalf of a user. Each action performed on behalf of the user (for example, execution of a task, transaction, or ECL statement) is a process. When a process executes within the address space of a subsystem, it acts with the subsystem's security attributes and can access objects as defined by that subsystem's security attributes. When a process references (calls) the address space of another subsystem, the operating system treats the referenced subsystem as an object and enforces security policy for access to that object. If security validations pass, a subsystem transition is allowed and the calling subsystem can enter the referenced subsystem to access.

Exhibit 10.8.33-2 (Cont. 7) (02-24-2022)
Terms and Acronyms

SVC	Supervisor Call
System Manager	The person currently responsible at the Service Centers who are responsible for the local computer systems. At the Computing Centers, the Branch Chiefs are generally considered to be the System Managers.
TCB	Trusted Computing Base
TCP/IP	Transmission Control Protocol/Internet Protocol
TD	Treasury Directive
TDP	Treasury Department Publication
TFTP	Trivial File Transfer Protocol
TIF	Tape Inventory File
TIGTA	Treasury Inspector General for Tax Administration
TPS	Trusted Privilege Set
TIP	Transaction Processing
TT&E	Test, Training, and Exercise
UACC	Universal Access
UNAX	Unauthorized access and inspection of taxpayer records
US-CERT	United States Computer Emergency Readiness Team
User	A person who is authorized to logon to a system in order to perform her/his assigned duties.
User Attributes	A characteristic of a user that defines the type of functions that a user can perform. The extraordinary privileges, restrictions, and processing environments assigned to a user. In RACF, the user attributes are SPECIAL, AUDITOR, CLAUTH, OPERATIONS, GRPACC, ADSP, and REVOKE.
UserID	A string of characters that uniquely identifies a user to a system.
VCM	Vanguard Configuration Manager Vanguard Manager
Version Control	The ability to match source code with executable code.
VTH	Virtual Tape Handler
Write	The ability to record information in an object. A subject writes into a memory location or copies to or transfers data onto mass storage or tape from main storage.

zOS RACF Terms and Acronyms	
ACEE (RACF)	Access Control Environment Element

Exhibit 10.8.33-2 (Cont. 8) (02-24-2022)
Terms and Acronyms

ACTIVE CLASSES (RACF)	The list of classes marked as ACTIVE via the SETROPTS command. Note that this resource class switch specifies for which classes RACF checking is in effect.
ALTER (RACF)	A level of access a group or individual may have. This access level allows the group members or individuals to read, copy, move, change or delete a partitioned, sequential or VSAM data set or read, copy, move, change or delete members within a partitioned dataset.
AUDIT (RACF)	This resource class switch specifies which classes RACF is to log every time a rule is created, changed, or deleted. Should be turned on for every resource class.
AUDITOR (RACF)	A system or group level attribute that gives the holder the ability to run specialized reports, monitor the system or group resources, and to set auditing features for others.
AUTH request (RACF)	The primary function of an AUTH request is to check a user's authorization to a RACF–protected resource or function. This is accomplished by issuing the RACROUTE macro with REQUEST=AUTH specified.
BACKUP RACF Database (RACF)	The database that is a carbon copy of the primary RACF database with all of the current RACF rules. It must be on a different DASD volume from the Primary RACF Database for security purposes in case there is a system crash or other problem(s).
BPXPRMxx (RACF)	The SYS1.PARMLIB member that contains the parameters that control the z/OS UNIX environment. It controls the way features work and it establishes logical access to data by configuring the HFS environment.
Cataloged Datasets Report (RACF)	DSMON report. See SYSCAT
CLAUTH (RACF)	Class Authority, granted to a RACF CLASS. This can be assigned to the USER class and to most any General Resource class. A user to whom CLAUTH has been assigned is authorized to create new profiles within that class.
CMDVIOL (RACF)	This setting causes an SMF (log) record to be written for every RACF command violation.
CONTROL (RACF)	This access authority grants a user the ability to define and delete VSAM datasets and is used for some resource profiles to give additional authority. It is one step lower than ALTER authority.
DFLTGRP (RACF)	Default Group
DSMON (RACF)	Data Security Monitor
ENHANCED GENERIC NAMING (RACF)	An option that determines whether *, **, or % may be used for dsnames. Always a good idea.

Exhibit 10.8.33-2 (Cont. 9) (02-24-2022)
Terms and Acronyms

Erase–on–Scratch (RACF)	An option which specifies whether a scratched disk dataset has zeros written over the data before the space is freed. Activate this option carefully as it can slow the system down because it uses so many resources to do an I/O with each zero written. Non Active = scratched datasets are overwritten. Active = all scratched datasets are overwritten. Security Level = only those scratched datasets with a specified security level or higher is overwritten. The IRS does not use security levels. RACF Rule = only those scratched datasets which have a RACF profile with the erase flag turned on.
EXECUTE (RACF)	Allows any users to load and execute, but not to read or copy programs.
FACILITY Class (RACF)	This resource class is used by various IBM and third party products.
Generic Profile (RACF)	A SETROPTS option which allows generic profiles, both dataset and resources, to be created. Valid characters which may be used in generic profiles are %, *, and **. A generic profile can protect one or more datasets or resources.
GENLIST (RACF)	A resource class switch which specifies classes for which RACF is to keep all generic profiles locked in memory.
Global Checking (RACF)	A resource class switch which specifies classes which RACF is to use the global checking list. Use for all datasets that are frequent used.
GLOBALAUDIT (RACF)	Type of access attempts, as specified by the GLOBALAUDIT operand, that shall be logged to the SMF dataset. In order to use this option user must have the AUDITOR attribute, either System or Group.
Group Tree Structure (RACF)	A list showing the hierarchy of all the groups on the system, including the superior or owner group and any subgroups.
ICHAUTAB (RACF)	The name of a load module, RACF Authorized Caller Table, created by the systems programmer that lists the names of programs authorized to issue RACF requests to perform user verification or to load RACF profiles into main storage. DSMON generated an auditor report on this module. One of the DSMON reports lists information on this module.
ICHRDSNT (RACF)	The name of a load module, RACF Dataset Name Table, created by the systems programmer that describes the primary and backup databases to RACF. It contains the name of the primary RACF database and the name of the backup RACF database.
ICHRIN03 (RACF)	The name of a load module, RACF Started Procedures Table, created by the systems programmer that lists the names of started tasks and their associated UserID and group. The STARTED class profiles take precedence over the entries in this table if RACF is running and STARTED class is in the ACTIVE class list.
ICHRMSFI (RACF)	The name of a load module, RACF Report Writer Exit Routine, created by the systems programmer that provides customized information to Report Writer; i.e., type of DASD on the system, the sort product that is to be used, etc.

Exhibit 10.8.33-2 (Cont. 10) (02-24-2022)
Terms and Acronyms

ICHRRCDE (RACF)	The name of a load module, RACF Class Descriptor Table for installation Classes, created by the systems programmer that provides a list of classes created by the installation and are not supplied by IBM. This table is used for RACF security by third party products; e.g. ENDEVOR. The name of the module reserved for the IBM classes is ICHRRCDX.
ICHRRNG (RACF)	The name of a load module, RACF Database Range Table, created the System Programmer that indicates whether a database has been split into parts for performance. It also defines which RACF profiles reside in each part based on the high–level qualifiers.
ICHSECOP (RACF)	The name of a load module provided with the product RACF, but is obsolete and should not be used. By coding and installing this module RACF initialization can be bypassed. This module can be used to control the number of resident control blocks if the site is not using ICHRDSNT and to disallow duplicate names for discrete profiles. Discrete profiles are not used on IRS systems.
ICS (RACF)	IBM Collaboration Solutions
INITSTATS (RACF)	This attribute allows the user record to be time–stamped at terminal sign–on or at the start of a batch job.
JES–BATCHALLRACF (RACF)	An option used to indicate that every batch job must have a RACF UserID associated with it. Activate at the same time as JES–XBMALLRACF.
JES–XBMALLRACF (RACF)	An option used to indicate that every batch job run under the JES execution batch monitor must have a RACF UserID associated with it. Activate at the same time as JES–BATCHALLRACF.
LOGOPTIONS (RACF)	This resource class switch specifies classes for which logging may or may not occur. ALWAYS = every access is logged, regardless of what's defined in the profile. NEVER = no accesses are logged. SUCCESSES = all successes are logged, in addition to whatever else may be defined in the profile. FAILURES = all failures are logged, in addition to whatever else may be defined in the profile. DEFAULT = logging is based on the RACF profile.
LPA (RACF)	Link Pack Area
MOUNT (RACF)	The parameter specifies data for a file system that is to be mounted by z/OS UNIX. There are usually multiple MOUNT statements and each can have a number of sub-parameters. The FILESYSTEM, SETUID|NOSETUID, and SECURITY|NOSECURITY sub-parameters have significant security considerations.
MVS (RACF)	Multiple Virtual Storage; is associated with the IBM Operating System and its products.
NDM (Network Data Mover) (RACF)	Also referred to officially as CONNECT:DIRECT. The process that is used to send data electronically through the network between systems and/or LPARs. The media can be 9 track tape, cartridge, DASD.

Exhibit 10.8.33-2 (Cont. 11) (02-24-2022)
Terms and Acronyms

NJE (Network Job Entry) (RACF)	The term used when submitting jobs on one system or LPAR and having them execute on another system or LPAR. It also covers the routing of print out to another system or LPAR.
OPERATIONS (RACF)	A System or Group attribute which grants ALTER access to all datasets or resources unless explicitly denied in the access list of a profile.
OPERAUDIT (RACF)	This attribute allows a log records to be written every time a user accomplishes an activity because that user has the OPERATIONS attribute.
OWNER (RACF)	The user or group who creates a profile or is named the owner of profile. The owner can modify, list, or delete the profile.
Primary/Backup RACF Dataset Report (RACF)	see RACDST
Primary RACF Database (RACF)	The database that has all of the current RACF rules. It must be on a different DASD volume from the Backup RACF Database for security purposes in case there is a system crash or other problem(s).
PRIVILEGED (RACF)	This is an attribute that can be associated with a Started Task in the STARTED Class or in the Started Procedures Table. The PRIVILEGED attribute allows a started task to bypass most authorization check
PPT (RACF)	Program Properties Table
Program Properties Table Report (RACF)	see SYSPPT
PROTECTALL (RACF)	An option that can be set to require a RACF profile covering any data set prior to allowing access to that data set.
RACAUT (RACF)	RACF Authorized Caller Table Report. This report is part of the DSMON run. It shows whether or not the system has an authorized caller table active with entries.
RACCDT (RACF)	RACF Class Descriptor Table Report. This report is part of the DSMON run. It shows all of the classes on the system, whether they are active or inactive, if audited, if statistics are kept, the UACC, and if operations is allowed.
RACDST (RACF)	Primary/Backup RACF dataset location report. This report is part the DSMON run. It shows both the primary and backup RACF databases. Additionally, the report shows the volume serial number, whether RACF indicated and/or protected, the UACC.
RACEXT (RACF)	RACF Exits Report. This report is part of the DSMON run. It shows whether or not there are any RACF exits that are active on the system.
RACF (Resource Access Control Facility) (RACF)	The IBM security software package
RACF Authorized Caller Table Report (RACF)	see RACAUT
RACF Class Descriptor Table Report (RACF)	see RACCDT

Exhibit 10.8.33-2 (Cont. 12) (02-24-2022)
Terms and Acronyms

RACF Exits Report (RACF)	see RACEXT
RACF Global Access Table Report (RACF)	see RACGAC
RACF Group Administrator	An individual, or group of individuals, who administers RACF security functions on a group level. These functions may include issuing passwords, etc., within the scope of the group.
RACF Group Tree Report (RACF)	see RACGRP
RACF Started Procedures Table Report (RACF)	see RACSPT
RACGAC (RACF)	RACF Global Access Table Report that shows dataset profiles that are defined in the Global Access Table that have been selected because the datasets protected have a high volume of access by system users. This table is stored in memory and bypasses RACF profile checking if requested access is less than or equal to access indicated in the Global Access Table. The use of this table enhances RACF performance.
RACGRP (RACF)	RACF Group Tree Report. This report is part of the DSMON run. It shows the hierarchy of all groups on the system and indicates the group ownership if other than the superior group.
RACHECK (RACF)	This function has been replaced by the AUTH request.
RACINIT (RACF)	A request which is used to verify the authority of a user to enter work into the system.
RACLIST (RACF)	This resource class switch specifies classes for which RACF is to keep all profiles locked in memory. Used for resource classes with few rules and frequent access or for classes requiring it.
RACSPT (RACF)	RACF Started Procedures Table Report. This report is part of the DSMON run. It shows all started procedures, the associated users and groups, and if privileged or trusted.
RACUSR (RACF)	Selected User Attribute Report. This report is part of the DSMON shows all of the users on the system who have either system or group level attributes of SPECIAL, OPERATIONS, or AUDITOR.
READ (RACF)	The authority to read or copy information.
ROOT (RACF)	The parameter specifies data for the file system that is to be mounted as the root file system for z/OS UNIX. It can have a number of sub-parameters; the FILESYSTEM and SETUID|NOSETUID sub-parameters have security considerations.
RSA (RACF Security Administrator) (RACF)	An individual, or group of individuals, who administers RACF security functions at the system level. These functions may include adding/deleting users, issuing passwords, creating dataset profiles, etc.
RUA (RACF User Administrator) (RACF)	An individual, or group of individuals, who generally processes the paperwork necessary to allow a user on a RACF protected system

Exhibit 10.8.33-2 (Cont. 13) (02-24-2022)
Terms and Acronyms

RVARY (RACF)	An option used to switch between the primary and backup RACF databases. This is always password protected.
SAUDIT (RACF)	A SETROPTS parameter, which turns on the logging of all RACF commands issued by users with the SYSTEM SPECIAL or Group SPECIAL attribute.
Security Level (RACF)	A classification of information defined by a sensitivity level. In RACF, an installation defined name that corresponds to a numerical security level (the higher the number, the higher the security level).
SETROPTS (RACF)	A RACF command used to set system–wide RACF options dynamically. Used for, but not limited to, establishing password rules, setting audit options on SPECIAL and OPERATIONS users, activating various RACF classes.
Single Level Name Prefix (RACF)	An option that specifies which prefix RACF is to use when DSNAMES have only one qualifier. This is only used for files on tape and cartridge. Single level file names are not allowed on DASD.
SPT (Started Procedures Table) (RACF)	The module name is ICHRIN03 and is sometimes known as the Started Task Table. This is a RACF controlled table that assigns a UserID and a group to a started procedure that can be used to determine RACF access authorities. It can assign RACF bypass privileges of PRIVILEGED or TRUSTED.
SPECIAL (RACF)	A System or Group level attribute which grants the user full control over all of the RACF profiles in the RACF database and allows for the issuance of all commands except auditing. Group SPECIAL only has this authority within the scope of the group.
Standard Access List (RACF)	A list within a RACF profile, showing all authorized groups and users and the access authority of each. The access list should contain only groups, SYSTEMIDs or other foreign UserIDs. Individual users who have additional responsibilities beyond their standard groups shall represent a special exception or situation.
STC (RACF)	Started Tasks
STARTUP_PROC (RACF)	The parameter specifies the name of the JCL procedure (PROC) that starts the z/OS UNIX component. This started task must be defined to the ACP. The name OMVS must be used.
STATISTICS (RACF)	This resource class switch specifies classes for which RACF is to keep reference counts for discrete profiles.
Status (RACF)	Refers to the state of the RACF primary and backup databases. A database can be set to active or inactive using the RVARY command. Since IRS Systems always have a primary and a backup RACF database, the RVARY command is not used to go into FAILSOFT processing.
STEPLIBLIST (RACF)	The parameter specifies the pathname of the HFS file that contains the list of MVS data sets that are used as step libraries for programs that have the set-user-id or set group id permission bit set.

Exhibit 10.8.33-2 (Cont. 14) (02-24-2022)
Terms and Acronyms

SUPERUSER (RACF)	The parameter specifies the UserID to be assigned to users when the su command is entered without a UserID operand. The UserID must be defined to the ACP as BPXROOT and have a UID of 0.
SUPGROUP (RACF)	Superior or owner group of any group
Switch (RACF)	This is accomplished by using the RVARY command to switch from using the primary RACF database the backup database or conversely.
SYS1.PARMLIB (RACF)	A critical system dataset that contains parameters used by the Operating System. It identifies the APF authorized libraries, Linklist libraries, SMF records the system is to record, system consoles, provides VTAM parameters and IPL information. The DSMON Utility uses information from this library for several of the reports it generates.
SYS1.UADS (RACF)	Only users defined in SYS1.UADS can use TSO when RACF is down for whatever reason. RACF does not validate those UserIDs, therefore, it is preferable to only have the RACF defined IBMUSER UserID in this dataset.
SYSAPF (RACF)	APF Authorized Datasets Report. This report is part of the DSMON run. It shows the Authorized Program Facility datasets along with the volume serial number, whether they are RACF indicated and/or protected, and the UACC.
SYSCAT (RACF)	Cataloged Dataset Report. This report is part of the DSMON and should be run weekly. It shows the master catalog and all associated user catalogs, along with the volume serial number, whether RACF indicated, and/or protected, and the UACC.
SYSLNK (Link Listed Datasets Report) (RACF)	This report is part of the DSMON run. It shows the datasets that are linklisted, along with the volume serial number, whether it is RACF indicated and/or protected, and the UACC.
SYSPPT (RACF)	Program Properties Table Report. This report is part of the DSMON run. It shows the program name, whether the program is able to bypass password protection, and whether it has a system key.
SYSSDS (RACF)	Selected Datasets Report. This report is part of the DSMON. It shows all of the selected dataset names, volume serial number, selection criterion, whether RACF indicated and/or protected, and the UACC.
System Report (RACF)	This report is part of the DSMON run. It shows the CPU–ID, Model Number, Name, version and release of operating system, Resident volume, SMS–ID, and the RACF version and release. This report is used to identify any changes that have been made to the operating system.
System Software RACF Specialists	System programmers working with RACF.
System UserIDs (RACF)	UserIDs that are not connected with an individual, but rather a started task. These tasks are critical to the Operating System or to the operation of the system; for example, UserIDs associated with JES2, VTAM and third party products.

Exhibit 10.8.33-2 (Cont. 15) (02-24-2022)
Terms and Acronyms

TAPE DATA SET PROTECTION (RACF)	An option that allows RACF to process tape datasets the same way that disk datasets are processed. Turn on unless there is a tape monitor such as Control–T.
TRUSTED (RACF)	This is an attribute that can be associated with a Started Task in the STARTED class or in the Started Procedures Table. The Trusted attribute allows for auditing, if requested, using the SETROPTS LOGOPTIONS command. A started task can be defined as PRIVILEGED, TRUSTED, or NONE.
TSO (RACF)	Time Sharing Option
TTYGROUP (RACF)	The parameter specifies the group name assigned to pseudo terminals (PTYs) and remote terminals (RTYs). The group must be defined to the ACP with a unique GID and users must not be assigned to this group. This group name is used by some shell commands (e.g., talk and write) when writing to the PTY or RTY being used by another user. The name TTY must be used.
UACC	Universal Access
UAUDIT (RACF)	An operand which when set on a user profile causes logging of ALL activity regardless of the global access table or SETROPTS log options. Can cause excessive logging and possibly loss of SMF data when enabled for users of Unix System Services.
UPDATE (RACF)	A user has the authority to add, change, or delete members from datasets.
USERIDALIASTABLE (RACF)	The parameter specifies the pathname of the HFS file that contains a list of UserIDs and group names with their corresponding alias names. The alias table is intended primarily for use where mixed or lower case UserIDs are used in the UNIX environment.
Violations Report (RACF)	A report that shows all security violations that were logged when a user attempted to access a resource or issue commands that were not authorized by RACF.
VRA (RACF)	Vanguard RACF Security Administrator
VTAM (RACF)	Virtual Telecommunications Access Method
WHEN (PROGRAM) (RACF)	This attribute allows program–pathing. For example, a user may update a dataset WHEN going through this specified program.

Unisys Terms and Acronyms	
CCB (Unisys)	Configured Common Bank
Clearance Level (Unisys)	A hierarchical classification for objects. Clearance levels can range from 0 through 63, with 63 being the most restrictive.

Exhibit 10.8.33-2 (Cont. 16) (02-24-2022)
Terms and Acronyms

Clearance Level Range (Unisys)	A range of clearance levels from which a user may choose from that determines the actions that can be executed on the system. The Unisys security administrator determines the range based on the Unisys Standard Access Matrix and specifies it in user security records.
Demand Run (Unisys)	A set of instructions users interactively enter at a terminal. Each control statement is usually processed before another one is entered.
Enforced Privilege (Unisys)	An override capability that is granted only to users who have the override capability (privilege) assigned in their user-id record, and only when the user-id is executing with the minimum clearance level specified for the privilege.
Executive (EXEC) (Unisys)	A software program that controls the system operating environment. The Executive processes user runs, controls files, manages system resources, and performs input/output operations for users. The Exec is the central component of the operating system and enforces security control.
Mandatory Access Validation (Unisys)	A means of controlling access to an object according to a set of validation rules for mandatory security attributes.
Non-human user-ids (Unisys)	User-ids used by scripts or other computer systems to establish sessions on the Unisys systems. Also user-ids used to run production/maintenance batch processing or to own subsystem files. Any user-id not associated with an individual.
Private (Unisys)	One of the categories of the discretionary mechanism access list. Only the owner can access a private object.
Public (Unisys)	One of the categories of the discretionary mechanism access list. The owner has all accesses to a public object. All other subjects have read, write, delete, and execute access.
Read (Unisys)	The ability to acquire information from main memory, a storage medium such as tape or disk, or an external device. Can also transfer data from one form of storage to another.
Residue security (Unisys)	The mechanisms, such as degaussing, used to ensure that sensitive data left in discarded files and tapes is not accessible to unauthorized users.
Security Level (Unisys)	The mandatory attributes of a subject or object. With Security Option 1, the security level is the executing clearance level for a subject and the clearance level for an object.
Security Option 1 (Unisys)	A separately installed feature that enhances the Fundamental Security feature. With Security Option 1, files are owned and data in files are protected by mandatory access control and discretionary access control.
Set A Privileges (Unisys)	Trusted security privileges that override all MAC and DAC security validations. These privileges include: SSCCL, SSBAFC, SSBYCOMP, and SSBYPASSOWNR.

Exhibit 10.8.33-2 (Cont. 17) (02-24-2022)
Terms and Acronyms

Set B Privileges (Unisys)	Trusted security privileges that allow users to override MAC and DAC security validations relating to devices, symbiont queues, tape volumes, and the MFD (such as would occur as a result of execution of a secured ER or execution of an ECL statement). Set B privileges are more concerned with system reliability, integrity, and resource use than they are with the global bypassing of MAC and DAC as with the set A privileges. Set B privileges include: SSBYCL, SSBYOBJREUSE, SSADID, SSBVOLCHK, SSSMOQUE, and SSDBACK.
System user-id (Unisys)	A user-id used by system software to access system resources.
TCB (Unisys)	Trusted Computing Base - The totality of protection mechanisms within the Unisys Operating System, including hardware, software, and firmware, which are responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system. The ability of the TCB to enforce a security policy depends solely on the mechanisms within the TCB and on the correct input of security-related entities (for example, a user's security level).
TPS (Unisys)	Trusted Privilege Set - Privileges override MAC and DAC and to circumvent security policy. These are to only be given to users or subsystems who are trusted not to violate security policy.
TST	Test system partition/environment on the Dorado used for testing of System Software
Unenforced Privilege/ Executive Request/ Interface (Unisys)	A system override capability that allows everyone to use the privilege/ executive request/interface.
Violation Report (Unisys)	A report that shows all security violations that occurred when a user attempted to access an unauthorized resource. Security related events are also reported.

Exhibit 10.8.33-3 (11-03-2023)
Related Resources

IRS Publications

- IRM 1.15.1 – *Records and Information Management, The Records and Information Management Program*
- IRM 1.15.2 – *Records and Information Management, Types of Records and their Life Cycles*
- 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 10.8.26 – *Information Technology (IT) Security, Government Furnished and Personally Owned Mobile Device Security Policy*
- IRM 10.8.50 – *Information Technology (IT) Security, Servicewide Security Patch Management*
- IRM 10.8.52 – *Information Technology (IT) Security, IRS Public Key Infrastructure (PKI) X.509 Certificate Policy*
- IRM 10.8.60 – *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*
- IRM 10.8.62 – *Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training and Exercise (TT&E) Program*

Department of the Treasury Publications

- Department of the Treasury TD P 85–01, Version 3.1.3 *Treasury Information Technology (IT) Security Program*, February 28, 2022

National Institute of Standards and Technology (NIST) Publications

- NIST FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems*
- NIST FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, September 20, 2018
- NIST SP 800-53 Rev 5, *Security and Privacy Controls for Information Systems and Organizations*, December 10, 2020
- NIST SP 800-53A Rev 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, January 25, 2022

Defense Information Systems Agency (DISA)

- DISA Mainframe Product Security Requirements Guide (SRG) V2R1
- Security Technical Implementation Guides (STIGS) are used as a basis for producing IRS Security Requirements Checklists. The security checklists are updated as DISA releases updated guidance and are posted on the IRS IT Cybersecurity Policy SharePoint site. The DISA version and release for each guide is contained within each checklist. Refer to the Security Requirement Checklists for additional information.
- DISA Security Requirements Guides and Security Technical Implementation Guides are available at: *https://public.cyber.mil/stigs/*

Other Publications
Committee on National Security Systems (CNSS) Glossary, Committee on National Security Systems Instruction (CNSSI) No. 4009