DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
2300/14
CP

From: Commandant of the Marine Corps

Subj: ENTERPRISE INFORMATION TECHNOLOGY SERVICE MANAGEMENT IDENTITY AND ACCESS MANAGEMENT PROCESS GUIDE

Ref: (a) MCO 5271.1B

Encl: (1) IRM-2300-14 Enterprise Information Technology Service Management Identity and Access Management Process Guide

1. PURPOSE. The purpose of the Enterprise Information Technology Service Management (ITSM) Identity and Access Management Process Guide is to establish a documented and clear foundation for process implementation and execution across the Marine Corps Enterprise Network (MCEN). Process implementation and execution at lower levels (e.g., Regional, Local and Programs of Record) must align and adhere to directives and schema documented within this guide. The use of this guide enables USMC Information Technology (IT) activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity.

2. CANCELLATION. N/A.

3. AUTHORITY. The information promulgated in this publication is based upon policy and guidance contained in reference (a).

4. APPLICABILITY. This publication is applicable to the Marine Corps Total Force.

5. SCOPE.

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is authorized.

b. Waivers. Waivers to the provisions of this publication will be authorized by the Director, Command, Control, Communications and Computers.

6. SPONSOR. The sponsor of this technical publication is HQMC ~~C4~~ CP.

K. J. NALLY
Brigadier General
U.S. Marine Corps
Director, Command, Control,
Communications and Computers (C4)

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

DISTRIBUTION: PCN 18623001400

Enterprise IT Service Management Identity and Access Management Process Guide

Release Date:
22 August 2014

Document Approval/Major Revision Change History Record

This table is used for initial release and subsequent revisions. Major revisions are indicated by the number to the left of the decimal point while minor revisions are indicated by the number to the right. Major revisions are required when the intent or process is changed rendering the prior version obsolete or when the number of minor releases total twenty (20). Changes to this document should be recorded, described and approved using the table below:

Release Date (MM/DD/YY)	Release No.	Approvals		Change Description
		Author	Process Owner/Approver	
12/xx/2013	0.1	Sarah Kang	Joe Rivera	Draft Release
		Printed Name	Printed Name	
06/05/2014	0.2	Sarah Kang	Joe Rivera	Initial Draft
		Printed Name	Printed Name	
08/01/2014	0.3	Sarah Kang	Joe Rivera	Updated per MCATS Tasker to Process Owners for documentation updates
		Printed Name	Printed Name	
08/06/2014	0.4	Sarah Kang	Joe Rivera	Added workflow in Appendix C-N
		Printed Name	Printed Name	
08/07/2014	0.5	Sarah Kang	Joe Rivera	Updated workflow in Appendix C-N
		Printed Name	Printed Name	
08/08/2014	0.6	Sarah Kang	Joe Rivera	Updated tables and workflow in Appendix C-N
		Printed Name	Printed Name	
8/22/2014	1.0	Sarah Kang	Joe Rivera	Initial Release
		Printed Name	Printed Name	
		Printed Name	Printed Name	

Table of Contents

Section	Title	Page
1.0	Introduction	1
1.1	Purpose	1
1.2	Scope	1
1.3	Process and Document Control	2
2.0	Process Overview	3
2.1	Purpose, Goals, and Objectives	3
2.2	Relationships with other Processes	3
2.2.1	Relationships with other Processes	4
2.3	High-Level Process Model	6
2.3.1	Identity and Access Management Process Description	7
2.4	Key Concepts	8
2.4.1	Commander's Critical Information Requirements	8
2.4.2	Access	8
2.4.3	Rights (or Privileges)	8
2.4.4	Support Groups	8
2.4.5	OU Control Groups	9
2.4.6	Directory Services	9
2.4.7	Human Resource Management	9
2.4.8	Service Request	9
2.4.9	Request for Change	9
2.4.10	Identity	9
2.4.11	Users, groups, roles and service accounts	10
2.4.11.1	Users	10
2.4.11.2	Authorized User	11
2.4.11.3	Privileged User	11
2.4.11.4	Identification and Authentication Management	11
2.4.11.4.1	Unique Identification	11
2.4.11.4.2	Authentication at Logon	12
2.4.11.4.3	Access to Authentication Data	12
2.4.11.4.4	User ID Reuse	12
2.4.11.4.5	User ID Removal	12
2.4.11.4.6	User ID Revalidation	12
2.4.11.4.7	Protection of Individual Authenticator	12
2.4.11.4.8	Protection of Individual Passwords	12
2.4.11.5	Personnel Security	13
2.4.12	Area of Responsibility (AOR)	13
2.4.13	Information Assurance (IA)	13
2.4.14	IA Training	13
2.4.15	Information Assurance Technicians (IATs) and Information Assurance Managers (IAMs)	13
2.4.16	Security Clearances	14
2.4.17	Confidentiality Level	16
2.4.18	Common Access Card	17
2.4.19	Support Tiers	17
2.4.20	Active Directory Permission	18
2.4.21	Access by Foreign Nationals	18
2.4.22	CAC Process including return of CAC:	22
2.4.23	Training Requirements:	26
2.4.24	Identity Management	27
2.4.25	Digital Signatures	27
2.4.26	Mission Assurance Categories (MAC)	27
2.4.27	Trusted Associate Sponsorship System (TASS)	28
2.4.28	Defense Enrollment Eligibility Reporting System (DEERS)	28

Section	Title	Page
2.4.29	Identity and Access Management (IdAM)	28
2.4.30	System Authorization Access Request (SAAR)	29
2.4.31	Certification and Accreditation	29
2.5	Quality Control	29
2.5.1	Metrics, Measurements and Continual Process Improvement	31
2.5.1.1	Critical Success Factors with Key Performance Indicators	32
3.0	Roles and Responsibilities	34
3.1	Responsibilities	38
4.0	Sub-Processes	40
4.1	Verification (sub-process 1.0)	40
4.2	Create New Account(s) (sub-process 2.0)	41
4.3	Change Access (sub-process 3.0)	43
4.4	Check and Monitor Identity Status (sub-process 4.0)	44
4.5	Log and Track (sub-process 5.0)	47
APPENDIX A — Acronyms		48
APPENDIX B — Glossary		49
APPENDIX C — Requesting .DA account workflow		55
APPENDIX D — requesting .EA account workflow		56
APPENDIX E — Requesting MCDSUS Authorized User Account workflow		57
APPENDIX F — Requesting .S.BPS Account workflow		58
APPENDIX G — Requesting .S.MCN Account workflow		59
APPENDIX H — Requesting .S.MIT Account workflow		60
APPENDIX I — Requesting .S.TSC Account workflow		61
APPENDIX J — Requesting .W.BPS Account workflow		62
APPENDIX K — Requesting .W.MCN Account workflow		63
APPENDIX L — Requesting .W.MIT Account workflow		64
APPENDIX M — Requesting .W.TSC Account workflow		65
APPENDIX N — Requesting .Z.MCN Account workflow		66
APPENDIX O — References		67

List of Tables

Table	Title	Page
Table 1-1.	Document Design Layers	2
Table 2-1:	Identity and Access Management Process Activity Descriptions	7
Table 2-2:	DoD Approved Baseline Certifications	14
Table 2-3:	Responsibilities, Clearance levels, and other Requirements for IT-I, IT-II, and IT-III	14
Table 2-4:	Limited Privileged Access - IT-II	15
Table 2-5:	Privileged Access - IT-I	16
Table 2-6:	PKI Certificate Issuance	16
Table 2-7:	IAM Objectives	32
Table 3-1:	Process Defined Roles and Responsibilities	35
Table 3-2:	RASCI Model for IAM by Process Role	39
Table 4-1:	Verification Sub-Process Descriptions	41
Table 4-2:	Create New Account(s) Sub-Process Descriptions	42
Table 4-3:	Change Access Sub-Process Descriptions	44
Table 4-4:	Check and Monitor Identity Status Sub-Process Descriptions	46
Table 4-5:	Log and Track Sub-Process Descriptions	47

List of Figures

Figure	Title	Page
Figure 1-1:	Process Document Continuum	1
Figure 2-1:	Identity and Access Management Relationships with other E-ITSM Processes	4
Figure 2-2:	High-Level Identity and Access Management Workflow	6
Figure 3-1:	Identity and Access Management Roles	35
Figure 4-1:	Verification Sub-Process	40
Figure 4-2:	Create New Account(s) Sub-Process	42
Figure 4-3:	Change Access Sub-Process	44
Figure 4-4:	Check and Monitor Identity Status Sub-Process	46
Figure 4-5:	Log and Track Sub-Process	47

1.0 INTRODUCTION

1.1 Purpose

The purpose of the Identity and Access Management (IAM) process guide is to establish a documented and clear foundation for process implementation and execution across the Marine Corps Enterprise Network (MCEN). Process implementation and execution at lower levels (e.g., Regional, Local, and Programs of Record) must align and adhere to directives and schema documented within this guide. The use of this guide enables USMC IT activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity as represented in Figure 1-1.

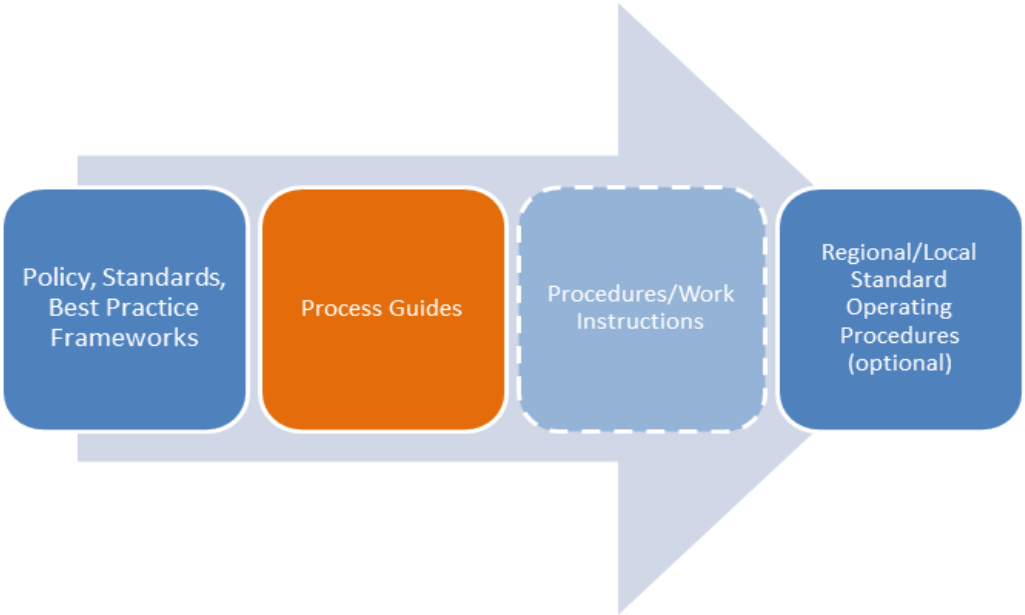


Figure 1-1: Process Document Continuum

1.2 Scope

The scope of this document covers all services provided in support of the MCEN for both the Secret Internet Protocol Router Network (SIPRNET), and the Non-Secure Internet Protocol Router Network (NIPRNET). Information remains relevant for the global operations and defense of the Marine Corps Enterprise Network (MCEN) as managed by Marine Corps Network Operations and Security Center (MCNOSC) including all Regional Network Operations and Security Centers (RNOSC) and Marine Air Ground Task Force Information Technology Support Center (MITSC) assets and supported Marine Expeditionary Forces (MEF), Supporting Establishments (SE) organizations, and Marine Corps Installation (MCI) commands.

Table 1-1 depicts the various layers of document design. Each layer has discrete entities, each with their own specific authority when it comes to promulgating documentation. This enterprise process operates at Level B, sub processes such as procedures and work instructions are not included within the scope of this document.

Table 1-1. Document Design Layers

	ENTITIES	DOCUMENTS GENERATED
LEVEL A	Federal Govt DoD DoN CMC/HQMC	Statutes/Laws DoD Issuances DoN Policies Marine Corps Orders/IRMS
LEVEL B	HQMC C4 MCNOSC MCSC	MCOs IRMs (Process Guides) Directives MARADMINS
LEVEL C	RNOSC MITSC	Regional Procedures Work Instructions
LEVEL D	MCBs POSTS STATIONS	Locally Generated SOP's

1.3 Process and Document Control

This document will be reviewed semi-annually for accuracy by the Process Owner with designated team members. Questions pertaining to the conduct of the process should be directed to the Process Owner. Suggested Changes to the process should be directed to USMC C4 CP in accordance with MCO 5271.1 Information Resource Management (IRM) Standards and Guidelines Program.

2.0 PROCESS OVERVIEW

2.1 Purpose, Goals, and Objectives

The purpose of the IAM process is to provide users with the appropriate level of access to services in accordance with policy defined in Information Security Management**.**

The primary goal of IAM is to manage access to services in accordance with organizational policies, responding efficiently to request to grant, modify or restrict access, while ensuring that the access rights provided are not improperly used.

The objectives of IAM include:

- Respond efficiently to requests for new access
- Ensure that access requests are properly reviewed and approved, confirming both the identity and access needs for each request
- Ensure that individuals are granted the appropriate level of access
- Monitor access to quickly identify misuse of access privileges
- Remove or update access when people change roles or jobs
- Report suspicious or unauthorized access
- Audit access to ensure the need to know and appropriate levels of access granted are in line with the current DD2875 SAAR on file

2.2 Relationships with other Processes

Many of the E-ITSM processes are interrelated. Identity and Access Management ensures the confidentiality, integrity, availability, authenticity, and non-repudiation of information is managed effectively across the enterprise and supports and interfaces with other processes. While any one of the E-ITSM processes can operate in the presence of an immature process, the efficiency and effectiveness of each is greatly enhanced by the maturity and integration of all E-ITSM processes.
Figure 2-1 depicts key relationships and dependencies that exist between the IAM process and current E-ITSM processes. These processes underpin the USMC near-term objectives. Note, Figure 2-1 is not all-encompassing and the relationships shown can de direct or indirect.

2.2.1 Relationships with other Processes

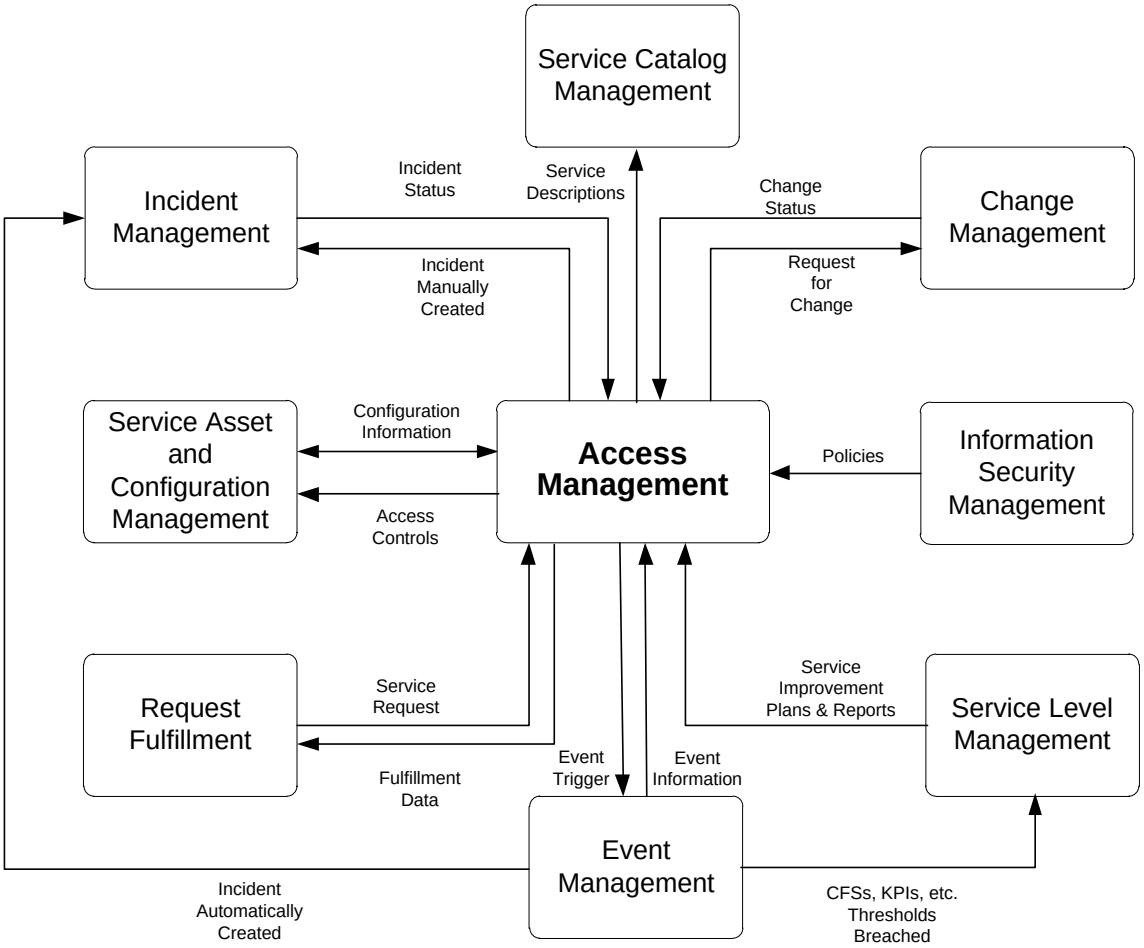


Figure 2-1: Identity and Access Management Relationships with other E-ITSM Processes

The following highlights the inputs and outputs regarding the relationship between the IAM process and other E-ITSM processes as shown in Figure 2.

Information Security Management

- Provides security and data protection policies that guide IAM, including the methods to verify user identity and confirm that they are entitled to the level of access being requested.
- IAM is involved in defining parameters for use in intrusion detection
- Provides the tools necessary to implement the policies.

Service Catalog Management

- Provides service descriptions and the means to access the services

Service Level Management (SLM)

Maintains the agreements for access to each service to include the criteria for who is entitled to access each service, what the cost of that access will be, if appropriate and what level of access will be granted to different types of user (e.g. managers or staff). Service Level Management feeds the criteria for Availability targets and goals.

Change Management

- Controls the actual requests for access. This is because any request for access to a service is a change, although it is usually processed as a Standard Change or Service Request once the criteria for access have been agreed through SLM.

Service Asset and Configuration Management (SACM)

- Provides information on CIs. The Configuration Management System (CMS) can be used for data storage and interrogated to determine current access details.

Request Fulfillment

- Provides the means by which users can request access to standard services.

Incident Management

- IAM provides IM with restricted information on incidents pertaining to inappropriate access.
- Provide a consistent repeatable process to track incidents to ensure:
    - Incidents are properly logged and routed and status is accurately reported
    - Queue of open/unresolved incidents are visible and reported
    - Incidents are properly prioritized and handled in the appropriate sequence
    - Resolution provided meets the defined Service Level requirements
- Dynamically assigning service resources to efficiently align IT work against mission objectives via incident prioritization
- Maintaining a constant and accurate link with the Service Desk (SD) function to continually improve the relationship between end users and IT operations

Event Management

- Constantly monitoring CIs and services, employing rules and filters to determine that a change in state or trends or patterns requiring action by IAM

2.3 High-Level Process Model

The following diagram illustrates the high level process model for Identity and Access Management.
See Section 4.0 for complete descriptions of the sub-process activities.

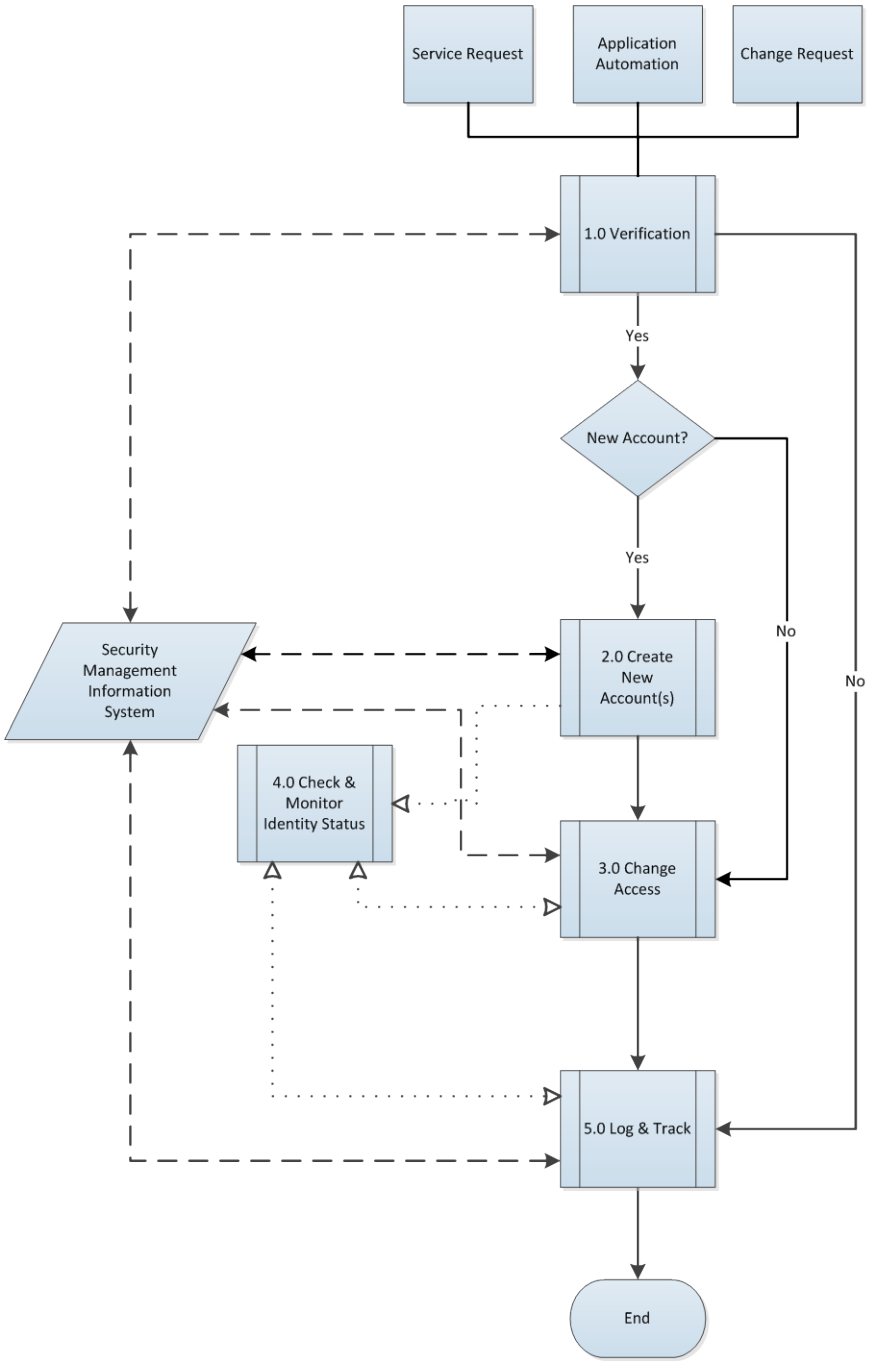


Figure 2-2: High-Level Identity and Access Management Workflow

2.3.1 Identity and Access Management Process Description

Identity and Access Management supports granting authorized and privileged users the rights to use services, while preventing or restricting access to non-authorized users. IAM does not define security standards; it solely and exclusively executes information security policies, and enables users to use the services documented in the service catalog.

Identity and Access Management performs five key activities – verification, request new account(s), change access, monitoring identity status, and log and track.

Table 2-1 below contains descriptions of each sub-process. As appropriate, sub-process numbers are hyperlinked to its detailed description in Section 4.0, Sub-Processes.

Table 2-1: Identity and Access Management Process Activity Descriptions

Number	Sub-Process	Description
1.0	Verification	An access request must be verified from two perspectives • The user for whom the access request is made is who they say they are. Users included in this Process Guide include Military, Contractors, Civilians, Volunteers, and Foreign Nationals. • The user for whom the access request is made has a legitimate requirement and authorization for the level of access being requested.
2.0	Request New Account(s)	Access is requested for new accounts, initiated by any of the following (Government Civilians, Military, Contractors, Volunteers, Foreign Nationals) through • A Service Request submitted through Request Fulfillment • When an individual is hired, promoted, transferred, or is leaving • An RFC • Application automation
3.0	Change Access	IAM may change access to include disabling and deleting accounts. Disabling and deleting access rights are based on policy, in the event of death, dismissal, resignation, role change such as add or remove access, logical moves, or in some cases, this generates requests to those supporting the service in order to facilitate the removal or restriction of rights. IAM may also restrict rights due to a role change or if an individual is under investigation (subject to policy). IAM does not decide who has access to which services, but executes the policies and regulations pertaining to access privileges. In most cases, this generates requests to those supporting the service. Role conflict may result when a user is assigned two roles which each preclude some aspect of the other role. IAM documents the conflict, and escalates it to the appropriate stakeholders for resolution.
4.0	Check and Monitor Identity Status	IAM should understand and document typical user role changes (e.g. job change or transfer). IAM tools should enable a user or group of users to be moved from one state to another, easily, and with an audit trail (DISA guidance, etc.).
5.0	Log and Track Access	IAM is responsible for ensuring that the rights provided are being properly used. Access monitoring and control are required in all technical and application management functions, and all service operation functions. Exceptions are handled by Incident Management

2.4 Key Concepts

The following key concepts are utilized extensively in the IAM Process.

2.4.1 Commander's Critical Information Requirements

Commander's Critical Information Requirements (CCIR) are the commander's "need to know immediately" information and response requirements. From MCWP 3-40.2 Information Management, "CCIR are tools for the commander to reduce information gaps generated by uncertainties that he may have concerning his own force, the threat, and/or the environment. They define the information required by the commander to better understand the battle-space, identify risks, and to make sound, timely decisions in order to retain the initiative. CCIR focus the staff on the type and form of quality information required by the commander, thereby reducing information needs to manageable amounts." In the context of Identity and Access Management, CCIRs are a basis for setting priority of Access requests.

All commands are required to produce command specific CCIR guidance with detailed IT service management requirements and are required to adhere to the current CCIR guidance of their superior commands. Common CCIR categories are Enterprise Service Management, Network Defense, Content Management, and MCEN, but others may be applicable based upon the commander's requirements.

2.4.2 Access

Access refers to the level and extent of a service's functionality or data that a user is entitled to use. Access refers to access and entry to services, data and facilities. IAM enforces the decision to restrict or to provide access, rather than deciding who has access to which IT services, it executes the security policies and regulations that have been defined.

Access is requested using one or more of the following mechanisms:

- A Request for Change
- A Service Request (submitted via the Request Fulfillment Process)
- Executing a pre-authorized script or option (application automation)

2.4.3 Rights (or Privileges)

Rights or Privileges refer to the actual active directory (AD) settings whereby a user is provided access to a service or a group of services. These are the rights or privileges which the user can exercise. Typical rights or levels of access include read, write, execute, change or delete. When a user is verified, Identity and Access Management will provide that user with rights to use the requested service.

2.4.4 Support Groups

Support Groups are AD Security Groups created to manage user access based on assigned roles. Support Groups are nested within the appropriate OU Control Group to inherit the appropriate roles based permissions assigned. The user can take on a number of roles and automatically inherits their rights on assignment to the appropriate Support Group. This simplifies the administration and overview of the distributed rights and increases their transparency. Users

performing similar activities generally use a similar set of services; it is more efficient to grant the user (or group of users) access to the whole set of services to which they are entitled at the same time. At no time should rights and permissions be directly assigned to a Support Group. Rights and permissions are inherited from nesting Support Groups into OU Control Groups.

2.4.5 OU Control Groups

Organizational Unit (OU) Control Groups are AD Security Groups that are mapped to roles based permissions which support a specific functional role or service. Rights and permissions are applied to these OU Control Groups to support assigning granular access control lists (ACLs) within AD. At no time should User Objects be directly nested within these OU Control Groups. Only Support Groups should be nested within OU Control Groups.

2.4.6 Directory Services

Directory Services describes a specific tool which can be used for the administration of identities, right, and roles. Directory Services is a directory of users and resources in a network. When sent a username, it returns the profile of the individual, which can include permissions for data access, as well as employee information. Directory services typically use hierarchical databases for fast lookups.

2.4.7 Human Resource Management

Human Resource Management is responsible for the process of hiring, promoting, relocating, terminating, or retiring. Identity and Access Management should be linked to the Human Resource processes to verify the users identify as well as to ensure that they are entitled to the services being requested.

2.4.8 Service Request

A Service Request is a formal request from a user for a particular service. An example is to obtain access to a shared drive. A Service Request is usually initiated through the Service Desk, or directly into the Request Fulfillment system, and executed by the relevant Technical or Application Management teams.

2.4.9 Request for Change

A Request for Change (RFC) is most frequently used for large scale service introductions or upgrades where the rights of a significant number of users need to be updated as part of the project.

2.4.10 Identity

Identity is used to grant rights or access to a user, person, or role. The identity of a user is the information about them that distinguishes them as an individual and which verifies their status within the organization. By definition, the identity of a user is unique to that user. Since there are cases where two users share a common piece of information (e.g., they have the same name), identity is usually established using more than one piece of information, for example:

- Name
- Address

- Contact details, e.g. telephone, e-mail address, etc.
- Physical documentation, e.g. driver's license
- Numbers that refer to a document or an entry in a database, e.g. employee number
- Expiration date (if relevant).

A user identity is provided to anyone with a legitimate requirement to access IT services or organizational information. The USMC will be faced with the need to provide access rights to temporary or occasional staff or contractors/suppliers. The management of access to such personnel often proves problematic – closing access after use is often as difficult to manage, or more so, than providing access initially. Well-defined procedures between IT and other stakeholders should be established that include fail-safe checks that ensure access rights are removed immediately if they are no longer justified or needed. Certain identifying items (including, but not necessarily limited to the Social Security Number and Birth Date) are considered Personally Identifiable Information (PII) and must be protected properly.

When a user is granted access to an application, it should already have been established by the USMC that the user is who they are.

2.4.11 Users, groups, roles and service accounts

While each user has an individual identity, and each IT service can be seen as an entity in its own right, it is often helpful to group them together so that they can be managed more easily. Sometimes the terms 'user profile' or 'user template' or 'user role' are used to describe this type of grouping.

However, most users also have some specialized role that they perform. For example, in addition to the standard services, the user may also perform a different role, that requires them to have access to some other tools and data.

Some groups may have unique requirements – such as field or home workers who may have to dial in or use Virtual Private Network (VPN) connections, with security implications that may have to be more tightly managed.

To make it easier for IAM to provide the appropriate rights, it uses a catalogue of all the roles in the organization and which services support each role. This catalogue of roles should be compiled and maintained by IAM in conjunction with HR and is oftentimes tied in or automated with Directory Services tools.

In addition to playing different roles, users may also belong to different groups. Identity and Access Management will assess all the roles that a user plays as well as the groups that they belong to and ensure that they provide rights to use all associated services.

2.4.11.1 Users

Individuals or system processes authorized to access an information system. Users are responsible for the protection of data they create and compliance with DoD and USMC IA policy requirements.

All users are responsible for the following:

(1) Compliance with the IS Security Program requirements.

(2) Being aware of and knowledgeable about their responsibilities in regard to IS security.

(3) Being accountable for their actions on an IS.

(4) Ensuring that any authentication mechanisms (including passwords) issued for the control of their access is not shared and is protected at the appropriate levels.

(5) Acknowledge, in writing, their responsibilities for the protection of the IS and classified information.

2.4.11.2 Authorized User

An Authorized User is any appropriately cleared individual with a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function. Authorized users are individuals who can input information to or modify information on an IS or who can receive information from an IS without a reliable human review. IAMs grant authorized users the rights to use a service.

2.4.11.3 Privileged User

A Privileged User is an authorized user who has access to system control, monitoring, or administration functions.

Privileged users have access to IS control, monitoring or administration functions. Examples include:

(1) Users having system administrator or equivalent access to a system (e.g., computer operators, ISSOs); users with near or complete control of an IS or who set up and administer user accounts and authenticators.

(2) Users having access to change control parameters (routing tables, path priorities, addresses, etc.) on routers, multiplexers, and other key infrastructure.

(3) Users who have been given the authority to control and change other users' access to data or program files (e.g., applications software administrators, administrators of specialty file systems, database managers).

(4) Users who have been given special access for troubleshooting or monitoring an IS' security functions (e.g., those using analyzers, management tools).

2.4.11.4 Identification and Authentication Management

As the complexity of a specific IS and the associated risk for this system increase, the need for identification and authentication of users and process becomes increasingly important.

Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system.

2.4.11.4.1 Unique Identification

Each user is uniquely identified and that identity is associated with all auditable actions taken by that individual. Each person within DoD is issued an electronic data interchange personal

identifier (EDIPI). This identification number is used as the individual's unique identifier for logical access and digital signature.

2.4.11.4.2 Authentication at Logon

Users are required to authenticate their identities at "logon" by supplying their credentials, such as a password, smart card, or biometrics, in conjunction with their user identification (ID) prior to the execution of anything on that system.

2.4.11.4.3 Access to Authentication Data

Access to data is restricted to authorized personnel through the use of encryption and file access controls.

2.4.11.4.4 User ID Reuse

Prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) needs to be removed from the system.

2.4.11.4.5 User ID Removal

When an employee terminates, loses access to the system for cause, or no longer has a reason to access the IS, that individual's user ID and its authentication is disabled or removed from the system.

2.4.11.4.6 User ID Revalidation

User IDs shall be validated on a quarterly basis to ensure ACLs and account access are accurate.

2.4.11.4.7 Protection of Individual Authenticator

It is the responsibility of the user to ensure they never share any personal credentials (password, pin, smartcard, token, etc.) with anyone for any reason.

2.4.11.4.8 Protection of Individual Passwords

When passwords are used as authenticators, the following applies:

(1) Passwords are protected at a level commensurate with the sensitivity level or classification level and classification category of the information to which they allow access.

(2) Passwords contain a minimum of eight non-blank characters, are valid for no longer than 12 months, and are changed when compromised.

(3) Password acceptability is based on the method of generation, the length of the password, password structure, and the size of the password space.

(4) When an IS cannot prevent a password from being echoed (e.g., in a half-duplex connection), an overprint mask is printed before the password is entered to conceal the typed password.

(5) User software, including operating system and other security-relevant software, comes with a few standard authenticators and passwords already enrolled in the system. The ISSO ensures that the passwords for all standard authenticators are changed before allowing the general user population access to the IS. The ISSO also ensures that these passwords are

changed after a new system version is installed or after other action is taken that might result in the restoration of these standard passwords.

2.4.11.5 Personnel Security

Duties, responsibilities, privileges, and specific limitations of IS users, both standard and privileged, are specified in writing. Security duties are distributed to preclude any one individual from adversely affecting operations or the integrity of the system.

Protection levels for particular IS are determined by the clearance level, formal access approvals, and need-to-know held by users of the IS, and the classification level of data processed or stored.

2.4.12 Area of Responsibility (AOR)

Area Of Responsibility (AOR) is used to define an area with specific or pre-defined operational boundaries where the USMC has the authority to plan and conduct operations and for which they bear certain responsibilities. Regional IAMs are responsible for their own AORs. Each of the 8 MITSC and MCEITS are responsible and accountable for their individual AORs.

2.4.13 Information Assurance (IA)

Information Assurance are measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

2.4.14 IA Training

All authorized users of USMC information systems must complete DoD IA approved training as a condition of access. Commanders of DoN Organizations may add to the standardized baseline training their specific DoN, Service, and local IA policies and procedures. DoD IA Training includes initial IA awareness orientation and annual IA awareness refresher training, along with those specific to job roles and functions. Personally Identifiable Information (PII) along with Information Assurance Awareness (IAA) is required IA Training for both Authorized and Privileged User Accounts. Information Assurance Policy and Technology (IAP&T) is required IA Training for Privileged User Accounts. Personnel in IA positions such as Authorizing Official (i.e., DAA), ISSM (i.e., IAM), ISSO (i.e., IAO), Computer Network Defense Service Provider (CNDSP) personnel, IA Security Architects and Engineers, and system administrator will have to be trained and certified to perform their duties to include IAW DODD 8570.01, “Information Assurance Training, Certification, and Workforce Management” and DOD 8570.01-M, “Information Assurance Workforce Improvement Program”.

2.4.15 Information Assurance Technicians (IATs) and Information Assurance Managers (IAMs)

Information Assurance Technicians (IATs) and Information Assurance Managers (IAMs) are the IA workforce that is responsible for protecting vital information, information systems and information infrastructures. To ensure that the IA workforce has the necessary skills and knowledge to accomplish this task, the DoD 8570.1 directive was put out to provide the guidance in making sure that the IA workforce took the necessary certifications. Personnel performing IA functions are required to take the certifications that are required for their position, category/specialty and level in order to fulfill the IA baseline certification requirement. Most IA levels within a category or specialty have more than one approved certification and a

certification may apply to more than one level. The below table defines each level for both IATs and IAMs that are required in regards to all DoD approved baseline certifications.

Table 2-2: DoD Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+ Network+ SSCP CCNA Security	GSEC Security+ SSCP CCNA Security	CISA CISSP (or Associate) GCED GCIH CASP
IAM Level I	**IAM Level II**	**IAM Level III**
CAP GSLC Security+	CAP GSLC CISM CISSP (or Associate) CASP	GSLC CISM CISSP (or Associate)

2.4.16 Security Clearances

Security clearances are granted to individuals allowing them to have access to classified information or restricted areas after the completion of a background check. There are several different levels of clearance to include: Controlled Unclassified, Confidential, Secret, Top Secret, and Sensitive Compartmented Information (SCI). Access to classified networks is suspended if an individual's security clearance is suspended, revoked, or denied. If denied, review circumstances to determine if continued access to unclassified systems is warranted and if revocation of the CAC is required (i.e. does not have a favorable NAC).

As per CNATRAINST 5230.4A, access to all DoD Information Systems are based on a demonstrated need to know, and granted in accordance with applicable laws and background investigations, special access and IT position designations and requirements. All persons assigned to sensitive positions or assigned to sensitive duties must be U.S. citizens. All personnel assigned to IT-I and IT-II positions, as well as all persons with access to controlled unclassified information (without regard to degree of IT access) or performing other duties that are considered "sensitive" must be U.S. citizens.

The table below depicts some of the responsibilities clearance levels, and other requirements as it pertains to personnel in the IT-I, IT-II, and IT-III categories.

Table 2-3: Responsibilities, Clearance levels, and other Requirements for IT-I, IT-II, and IT-III

	IT-I	IT-II	IT-III
Responsibilities include: (not all inclusive)	Responsibility or development and administration of Government computer security programs, including direction and control of risk analysis and/or threat assessment. Significant involvement in life-critical or mission-critical systems. Responsibility for the preparation or approval of data into a system, which does not necessarily involve	Responsibility for systems design, operation, testing, and/or monitoring that is carried out under technical review of higher authority in the IT-I category include: Access to and/or processing of proprietary data,	Incumbents in this position have non-privileged access to one or more DOD information systems/applications or database to which they are authorized access.

	personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain. Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10M per year or grater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the IT-I category to ensure the integrity of the system. Positions involving major responsibility for the direction, planning design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software. Other positions as designated by DON that involve relatively high risk for effecting grave damage or realizing significant personal gain.	information requiring protection under the Privacy Act of 1974, and Government – developed privileged information involving the award of contracts. Accounting, disbursement, or authorization from system of dollar amounts less than $10M per year. Other positions are designated by DON that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in the IT-I position.	
Clearance	SSBI or SSBI-PR (updated every 5 years) NAC	NAC	NAC
Miscellaneous	Must be US citizen	Must be US citizen	FN or US citizen

The tables below depict the investigative levels for users with IA Management access to DoD Unclassified Information Systems for Limited Privileged Access (IT-II), Privileged Access (IT-I) and PKI Certificate Issuance. The assignment to privileged user roles with IA management access is outlined in the below table.

Table 2-4: Limited Privileged Access - IT-II

Limited Privileged Access (IT-II)	Foreign National (FN)	US Civilian	US Military	US Contractor	Conditions or Examples
IAM (with no IA admin. privileges)	Not allowed	NACI	NACLC	NACLC	
IAO (with no IA admin. privileges)	Conditionally allowed – NACLC – (equivalent)	NACI	NACLC	NACLC	FN – with DAA written approval, direct or indirect hires may continue as IAOs until replaced, provided they serve under the immediate supervision of a US citizen IAM, and have no supervisory duties
Supervisor of IT-II or IT-I positions	Not allowed	NACI	NACLC	NACLC	
Administrator (with no IA admin. privileges)	Allowed – NACLC – (equivalent)	NACI	NACLC	NACLC	FN –under the immediate supervision of a US citizen
Maintenance of	Conditionally	NACI	NACLC	NACLC	

IA-enabled products	allowed – NACLC - (equivalent)				

Table 2-5: Privileged Access - IT-I

Privileged Access (IT-I)	Foreign National (FN)	US Civilian	US Military	US Contractor	Conditions or Examples
DAA or IAM	Not allowed	SSBI	SSBI	SSBI	
IAO (with IA admin. privileges)	Conditionally allowed –SSBI– (equivalent)	SSBI	SSBI	SSBI	FN – with DAA written approval, direct or indirect hires may continue as IAOs until replaced, provided they serve under the immediate supervision of a US citizen IAM, and have no supervisory duties
Monitoring and Testing	Not allowed	SSBI	SSBI	SSBI	
Administrator (with IA administrative privileges)	Conditionally Allowed - SSBI - (equivalent)	SSBI	SSBI	SSBI	Examples: Administration of IA devices (e.g., boundary devices, IDS, routers and switches) FN - Under the immediate supervision of a U.S. citizen, and with written approval of the Head of the DoD Component
Maintenance of IA products	Conditionally Allowed - SSBI - (equivalent)	SSBI	SSBI	SSBI	FN - Under the immediate supervision of a U.S. citizen, and with written approval of the Head of the DoD Component All - Also subject to IA controls (e.g., PEPF and ECRB)

Table 2-6: PKI Certificate Issuance

User Roles	Foreign National	US Civilian	US Military	US Contractor
Unclassified and Classified (Secret and Below) Certificate Issuance (IT-II)	Not allowed	NACI	NCALC	NACLC
Classified (Above Secret) Certificate Issuance (IT-I)	Not allowed	SSBI	SSBI	SSBI

2.4.17 Confidentiality Level

Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The Department of Defense has three defined confidentiality levels: Classified, Sensitive, and Public. Classified information is material that is sensitive information that requires protection of confidentiality, integrity, or availability. Access is restricted to particular groups of people, and mishandling can incur criminal penalties and loss of respect. A formal security clearance is usually required in order to be able to handle classified documents or have access to

classified data. Sensitive information or knowledge requires control of access in order to deter the loss of an advantage or level of security if disclosed to others. Loss, misuse, modification, or unauthorized access to sensitive information can adversely affect the privacy or welfare of an individual, or even the security, internal and foreign affairs of a nation depending on the level of sensitivity and nature of the information. Public information refers to information that is already of public record or knowledge. Access to or release of public information may be requested by any member of the public. 5. Network Administrators of Unclassified Networks are required to have Secret clearances, and loss of that clearance requires suspension of administrator privileges on the network.

2.4.18 Common Access Card

The Common Access Card (CAC) is the primary identity credential supporting interoperable physical access to DoN installations, facilities, buildings, controlled spaces, and logon access to all unclassified DoN networks. CAC eligibility pertains to all of the groups identified below:

- All Active Duty Military, Selected Reserve Personnel, Government Civil Service, and Full Time Non-Appropriated Funds (NAF) employees
- Contractors on a current USMC Contract Delivery Order who meet one or more of the following criteria
    - Provisioned with a MCEN account
    - By Statement of Work, requires access to disparate installations weekly within a geographic region
    - Requires a Geneva Conventions (GC) ID and meets DODI 3020.41 requirements
    - Employed and residing in a foreign country for a period of at least 365 days
- Foreign National affiliates who meet eligibility requirements

If adjudication is not positive via a minimum background security investigation of a National Agency Check with Inquiries (NACI), or DoD approved equivalent, then the CAC must be immediately revoked or retrieved. Final investigation adjudication must be verified through the Joint Personnel Adjudication System (JPAS). Trusted Association Sponsorship System (TASS) Trusted Agents (TAs) are responsible for verification of background vetting before approving a TASS record. Eligible contractors will be issued the CAC for the length of the contract, base year plus option years not to exceed three years regardless of contract funding status. Finally, the CAC must be issued via a strong security and vetting process. This process requires a separation of roles for the sponsoring, vetting, and issuance of credentials for personnel.

2.4.19 Support Tiers

These Support Tiers are established to support Incident Management (IM) ticket escalation and resolution.

Tier 1 = Help Desk (ESD [MITSC, B/P/S, T/S/C])

Tier 2 = Regional Support (MITSC, B/P/S, T/S/C)

Tier 3 = Enterprise Support (MCNOSC)

Tier 4 = Vender Support (Technology Vender)

2.4.20 Active Directory Permission

Based on the IRM 5231-2, IRM 5231 Implementation guide, TASKORD14-018, and FRAGO 08 we have established the following privileged account types/roles within the MCDSUS Domain:

Org Level	Type/Role	Extension	Clearance	8570 Training
Enterprise	Enterprise Admin	.ea	SSBI	IAT Level III
Domain	Domain Admin	.da	SSBI	IAT Level III
MCNOSC	MCNOSC Admin	.z.mcn	SSBI	IAT Level III
MCNOSC	MCNOSC Admin	.s.mcn	NACLC	IAT Level II
MCNOSC	MCNOSC Admin	.w.mcn	NACLC	IAT Level I
MITSC	MITSC Admin	.s.mit	NACLC	IAT Level II
MITSC	MITSC Admin	.w.mit	NACLC	IAT Level I
Base	Base Admin	.s.bps	NACLC	IAT Level II
Base	Base Admin	.w.bps	NACLC	IAT Level I
Tenant	Tenant Admin	.s.tsc	NACLC	IAT Level II
Tenant	Tenant Admin	.w.tsc	NACLC	IAT Level I

2.4.21 Access by Foreign Nationals

Commanders of DoN Organizations control access to DoN Information systems and networks in accordance with relevant national and DoD policies and guidance. Access to DoN Information systems and networks will be based on a demonstrated “need to know”. Foreign exchange personnel and representatives of foreign nations, coalitions, or international organizations may be authorized access to DoN Information systems and networks containing classified information or information that could be considered Controlled Unclassified Information (CUI), to include sensitive information only if all applicable references and requirements are met. DoN information systems and networks need to be sanitized and/or reconfigured to prevent unauthorized access to classified and CUI by foreign nationals. Access should be regulated through the use of positive technical controls such as a Demilitarized Zone (DMZ) and ensuring Web sites are properly configured to grant access to only authorized personnel. Foreign nationals also need to be identified in DoN e-mail addresses, e-mail display names, along with automated signature blocks. It is required by Foreign Nationals to have their email identified with a two character country code and may require special forms to in order to grant access rights. Any further questions regarding the process, policy, and negotiation regarding Foreign Nationals should be directed to C4 Cyber Security (CY).

The following information is extracted from DODI 8500.2 and DODD 8500.01E:

- Individual foreign nationals may be granted access to specific classified U.S. networks and systems as specifically authorized under Information Sharing guidance outlined in changes to National Disclosure Policy (NDP-1).
    - Classified ISs are sanitized or configured to guarantee that foreign nationals have access only to classified information that has been authorized for disclosure to the foreign national’s government or coalition, and is necessary to fulfill the terms of their assignments.

- U.S.-only classified workstations are under strict control at all times. Individual foreign nationals (e.g., foreign exchange officers) may be granted access to unclassified U.S. networks and systems (e.g., Non-Secure Internet Protocol Router Network (NIPRNET)) for official purposes by CC/S/As IAW DODI 8500.2.
- Contractors including Federally Funded Research and Development Center (FFRDC) personnel -- and foreign nationals granted e-mail privileges DOD systems are clearly identified as such in their e-mail addresses.

The following information is extracted from the CJCSI 6510.01F:

Foreign Access CC/S/As is responsible to:

- Control access by foreign nationals (i.e., non-U.S. citizen) to DOD-owned or DOD-operated IS, including ISs or networks operated by contractors under a DOD contract. Controls must prevent unauthorized (intentional or unintentional) access, disclosure, destruction, or modification to the information or the IS.
- Limit foreign national access to classified information (including classified information received from DOD classified systems) to foreign governments or organizations IAW applicable laws and policies including National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems" NSTISSP 8, "National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments"; NDP-1 (reference u); DODD 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"; DODD 5230.20, "Visits and Assignments of Foreign Nationals"; and CJCSI 5221.01.
- Ensure that foreign nationals only access "CUI" authorized for release to the foreign national's government. Access by foreign nationals to CUI are IAW applicable laws and policies including National Security Directive 42; NSTISSP 8; the International Traffic in Arms Regulations (ITAR); the Export Administration Regulations (EAR); DODD 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure"; and DODD 5400.7, "DoD Freedom of Information Act (FOIA) Program".
- Foreign National Access to Information Systems. CC/S/As is responsible to:
    - Authorize access to DOD-owned or DOD-managed ISs with CUI on a need-to-know basis for official duties by foreign nationals (e.g., DOD foreign national employees (direct and indirect hires) or military, civilian, or contract employees of foreign governments serving with DOD).
    - Authorize access to U.S. classified ISs and workstations as specifically authorized under Information Sharing guidance outlined in changes to NDP-1.
    - Issue eligible foreign nationals a CAC IAW DTM 08-003, "Next Generation Common Access Card (CAC) Implementation Guidance" and DODI 1000.13. Eligibility is based on DOD government sponsorship. A CAC may be issued when the non-U.S. person meets the requirements of paragraph 3.a.(3) IAW DODI 1000.13. Visiting and assigned foreign nationals must possess a visit status and

security assurance that has been confirmed, documented, and processed IAW international agreements and DODD 5230.20.

- Access Requirements. Before authorizing foreign nationals access to specific ISs, CC/S/As is responsible to:
  - Approve foreign national access to unclassified IS (e.g., NIPRNET). This approval authority is delegated to CC/S/A Headquarters.
  - Approve foreign national access to U.S. classified ISs as specifically authorized under Information Sharing guidance outlined in changes to NDP-1.
  - Ensure CC/S/A designated official(s) authorized to grant a foreign national access are designated.
  - Identify sponsors for all approved IS access by foreign nationals and provide to the Authorizing Official (i.e., DAA) with appropriate control measures identified to protect information.
  - Ensure foreign national employees meet the same or equivalent requirements as all DOD authorized users (i.e., military, and DOD government civilian and contract employees) for access to DOD ISs and networks.
  - Ensure a foreign national employee covered by a Status of Forces Agreement (SOFA) with privileged (IA Management) access for unclassified ISs receives a host-nation personnel security investigation that is the equivalent of the U.S. investigative level IAW DODI 8500.2.
  - Include in contracts a data item description for meeting security requirements in DOD 5200.2-R.
  - The Authorizing Official (i.e., DAA) is responsible to:
    - Ensure system certification and accreditation documentation is updated to reflect foreign national access.
    - Ensure accountability is maintained through audit trails of all actions taken by foreign nationals within ISs.
    - Ensure foreign users sign a user agreement and receive initial IA awareness training prior to gaining access. User agreement will outline DOD and local IS security policies and procedures and consequences of misuse.
    - Ensure the ISSM (i.e., IAM) is given authority to enforce policies and revoke access if deemed necessary.
    - Ensure that the foreign national is identified when dealing with others through written and electronic communications, such as e-mail.
  - Ensure the following minimum controls are implemented for foreign nationals:
    - Ensure workstations accessed by foreign nationals can be logically grouped and managed (e.g., virtual LAN, static IP address or Dynamic Host Configuration Protocol (DHCP)).

        - Disable modem ports, CD drives, USB ports, and unused network interface cards (NICs).
        - Port security is enabled IAW DOD Access Control STIG.
        - Establish Active Directory Organizational Unit specifically for foreign nationals.
        - Prevent foreign nationals from accessing U.S.-only public folders.
    - Ensure user name for e-mail accounts includes individual's nationality. If a commander or agency head determines operational and/or security concerns preclude use of specific nationality for an individual, then generic designation of "FN" (foreign national) will be used and documented. U.S. military and government employees who are lawful permanent residents do not need to include nationality for user name on unclassified e-mail accounts.

      Format is as follows:

        - Use the federal information processing standard International Organization for Standardization (ISO) 3166, "Country Codes" alpha-2 codes for country designations in the Simple Message Transfer Protocol (SMTP) address.
        - The alias format is name, country, and duty description and the SMTP format is name.ISO alpha-2 countrycode@CC/S/A.mil. Format examples: Alias -- John Doe, AU, LNO, Combatant Command SMTP -- John.Doe.AU@combatant command.mil. Alias -- John Smith, GB, Foreign Liaison Officer (FLO), Service SMTP -- John.Smith.GB@service.mil.
        - Use auto e-mail signature blocks including foreign individual's name, country, duty description, and organization assigned. Format example: Doe, John WG CDR, Australia -- FLO, Combatant Command, J-6.

- Foreign National Access to U.S.-Only Workstations and Network Equipment. CC/S/As is responsible to:
    - Maintain strict U.S. control of U.S.-only workstations and network equipment at all times.
    - Group U.S.-only workstations together in a U.S.-controlled workstation space when workstations are located in workspaces physically accessible by foreign nationals (such as combined operations centers).
    - If the grouping of U.S.-only workstations at a site is not operationally possible, the following steps be taken by the responsible CC/S/A element:
        - The U.S. command or agency authorizes an exception at the site, in writing, stating operational reasons for exception, and maintain the record of exception.
        - Develop, publish, and maintain specific site written procedures on security measures to safeguard U.S.-only classified workstations.
        - Ensure that U.S. personnel are briefed and enforce security measures.
    - Announce presence. If a foreign national is permitted access to U.S.- controlled workstation space, the individual must be announced, must wear a badge clearly

identifying him or her as a foreign national, and must be escorted at all times. In addition, a warning light must be activated if available and screens must be covered or blanked.

- If the foreign national is permitted to view the screen, U.S. personnel must ensure:
  - Information is releasable in accordance with CC/S/A guidance and is consistent with NDP-1; DODD 5230.11; DODD 5230.20; DOD 5200.1-R; and CJCSI 5221.01.
  - Check with organization security office to ensure foreign national has security clearances granted by his or her government at a level equal to that of the classified information involved and an official need-to-know.

Access by Contractors:

2.4.22 CAC Process including return of CAC:

1. Prime Contractor or Subcontractor Supervisor identifies employee(s) requiring a CAC for logical and physical access. Contractor and Subcontractors submit requests to Contractor FSO.
2. Contractor FSO verifies employee's data and clearance status through the Joint Personnel Adjudication System (JPAS) and sends encrypted applicant info to Trusted Agent (TA).
3. 3. TA checks status of applicant's background check in JP AS. The TA forwards the applicant info to Trusted Agent Security Manger (T ASM), via an encrypted email, for a background check and verifies data and length of contract are accurate.
4. The National Crime Information Center (NCIC) conducts a background check. The TA queries the Commander, Naval Region Mid Atlantic (CNRMA) database for "clear" or "denied" status. If the applicant is cleared then the TA forwards employee user ID's and temporary passwords to Contractor FSO via an encrypted email. Contractor FSO provides that information to the employees. If the applicant is not cleared, the T A notifies Contractor FSO of denial, not directly to applicant. Contractor provides denial notifications to their employee or the employing Company.
5. Once the applicant has received a temporary ID and password, the applicant completes the application in Trusted Associate Sponsorship System (TASS). Normal communication between TA and applicant is managed automatically via TASS; however, if there is an issue or a question, TA will notify applicant via email.
6. The TA reviews the application for completeness and submits to CNRMA via TASS. If The TA finds that the application is not complete, and then the application is returned to the applicant. Upon approval, the applicant receives notification of approval and proceeds to the nearest RAPIDS station with two forms of valid ID to pick up CAC.
7. At the RAPIDS station, the RAPIDS agent validates the identity of the applicant and issues the CAC card
8. Upon completion of assignment, or for any other reason that the employee must terminate access to facilities, sensitive or classified information, and systems, the Contractor FSO must ensure that the CAC is revoked and returned within 5 days (per the

DD-254). The Contractor FSO must turn the expired or revoked CAC in to the DON. If termination or removal from the worksite is for any adverse reason, clearance revocation, or security violation, the Industrial Security Officer (ISO), FSO, or Site Manager will provide an explanation to Program Security. Note: The Contractor FSO must notify the TA to revoke an employee's CAC in TASS.

9. If employee needs to renew their CAC begin the process from step 3.2. The original CAC will be collected by the CAC office upon issuance of the new CAC. If the contractor is assigned to a new contract, and the new contract expiration date is prior to the CAC expiration date, a new CAC is not required.

10. If a CAC is lost or stolen, the Contractor FSO shall notify the TA and the T A immediately revokes the CAC in TASS. The FSO shall also present documentation to the TA confirming that the ID card has been reported lost or stolen. If a replacement CAC is required, contractor initiate's a CAC request as a new request and the employee screening process is the same as for the initial CAC request.

Security Clearance Process: This Security Clearance process includes a government requirement for a cleared person to perform duties on the enterprise contract, the flow of procedures to obtain and maintain a security clearance, and procedures at the termination of the clearance or transfer from the Contractor program.

1. An employee is hired to work at a site requiring a personnel security clearance (PCL). The Prime (or Subcontractor) Company Facility Security Officer (FSO) checks Joint Personnel Adjudication System (JPAS) for a current security clearance, or has the employee begin the security clearance application. [NOTE: A facility clearance (FCL) and FSO is required for any company supporting the contract with cleared personnel]

2. If the employee has a current security clearance at the level required for the work, the Company Facility Security Officer (FSO) sends a Visit Authorization Letter (VAL) to the FSO for the new employee's work site. The receiving FSO notifies the Contractor supervisor or government lead that the employee is cleared for work.

3. If the employee does not have a clearance or if the clearance is out of date, the Company FSO initiates a Personal Security Investigation (PSI) in JP AS.

4. The employee completes an SF-86 via e-QIP.

5. The FSO reviews the SF-86 and when complete, releases the SF-86 to Defense Security Service (DSS) via JP AS.

6. DSS reviews the SF-86 and initiates the appropriate investigations based on the clearance level required.

7. DSS then submits the SF-86 to the Office of Personnel Management (OPM) for review and investigation.

8. OPM completes the investigation and submits the results to the Department of Defense Central Adjudication Facility for adjudication. If favorable, JP AS is annotated for a "Final" or "Interim clearance status.

9. If granted an interim clearance and the final clearance determination is unfavorable, the clearance will be cancelled.

10. The FSO will have to proactively check the JP AS system for updates to a clearance that is under consideration.
11. If an employee is working in a cleared capacity and their clearance is denied, the FSO must immediately notify the employee's government lead to begin out-processing of the employee.
12. The Contractor FSO ensures that employee executes a Classified Information Nondisclosure Agreement (SF 312) prior to gaining initial access to classified information and FSO records execution of the SF 312.
13. Upon completion of assignment, or for any other reason that the employee must terminate their security clearance, the company FSO must update JP AS and complete any site-specific processing. FSO ensures that employee signs Security Debriefing Acknowledgement on the SF 312 and the Security Termination Statement.
14. If termination or removal from the worksite is for any derogatory reason, clearance revocation, or security violation, the FSO or Site Manager will provide an explanation to Program Security.

IT Level Process: This process includes identification of IT Level access need, generation of a request, designation of an employee to the IT Level need, training, granting of access, and removal of access.

1. Contractor has a need for an IT level position and the Contractor manager submits a Request for Access (RF A) form to the local Security Office.
2. IT level is assigned according to the DD 254, which provides the criteria for each IT level. Contractor notifies Program Office of the IT level assigned to a person.
3. The individual and the Contractor Industrial Security Office (ISO) complete a Standard Form (SF) 85P for a trustworthiness investigation or a SF 86 for security clearance.
4. If no issues are discovered in the background investigation, a "Favorable Determination" is entered in JPAS. Contractor ISO checks for trustworthiness determination or clearance level in Joint Personnel Adjudication System (JPAS).
5. Contractor ISO verifies that the individual has a "need-to-know".
6. Contractor ISO checks the individual has completed the required Information Assurance (IA) Workforce Training and any necessary certifications for the designated IT level.
7. If need to know and necessary certifications are verified, the individual is granted an IT Level access.
8. If employee is being assigned to an IT-I or IT-II positions, the contractor Information Assurance Manager (lAM) verifies the individual's assignment.
9. Once the individual has assumed the IT position, he or she must complete IA Refresher Training and must participate in the Continuous Evaluation Program (CEP).
10. Upon departure from the position, the Contractor cancels the IT level certification and terminates access.

Security Reporting:

Security reporting includes any communications regarding the contract security status.

1. Information coming to the contractor's attention concerning actual, probable or possible

espionage, sabotage, terrorism, or subversive activities at any of its locations.

2. Efforts by any individual, regardless of the nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee.
3. The possibility that access to classified information in the future has been reasonably foreclosed.
4. Adverse information regarding any cleared employees.
5. An employee who no longer wishes to be processed for a clearance or no longer wishes to continue an existing clearance.
6. Refusal by an employee to execute the SF-312, "Classified Information Nondisclosure Agreement".
7. The unauthorized receipt or discovery of any classified material. Reports of loss, compromise, or suspected compromise of classified information.
8. Individual culpability regarding deliberate disregard of security requirements, violation involving gross negligence in the handling of classified material, and violations involving a pattern of negligence or carelessness.
9. If classified material is inadvertently distributed outside the facility without the proper classification assigned to it or without any markings to identify the material as classified.
10. If a non-U.S. citizen employee granted a Limited Access Authorization (LAA) becomes a citizen through naturalization.
11. Change Conditions Affecting the Facility Clearance:

- Any change to the information previously submitted for key management personnel.
- Any action to terminate business or operations for any reason, imminent adjudication or reorganization in bankruptcy, or any change that might affect the validity of the Facility Clearance.
- Any change concerning the information previously reported by the contractor concerning foreign ownership, control or influence.
- Any change in a facility's storage capability that would raise or lower the level of classified information the facility is approved to safeguard.
- Any emergency situation that renders the facility incapable of safeguarding classified materials.
- Significant vulnerabilities identified in security equipment, intrusion detection systems (IDS), access control systems, communications security (COMSEC) equipment or systems, and information systems (IS) security hardware and software used to protect classified material.
- Information System security incidents identified through self-inspection program.
- Unauthorized disclosure involving Restricted Data (RD) and Formerly Restricted Data (FRD).
- Receipt of classified material from foreign interests that is not received through government channels.
- Violation of procedures regarding storage, custody, and control of classified information abroad by employees of a U.S. contractor.

2.4.23 Training Requirements:

Introduction to Personnel Security

Description: This course introduces the management practices and procedures required to administer the Department of Defense (DoD) Personnel Security Program (PSP) at the military base/installation level. The course provides an overview of the elements of the PSP to include: designation of sensitive duties; investigative and adjudicative practices; security officer responsibilities under the PSP one-time access requirements; special security program requirements; and due process procedures. The course identifies the types of personnel security investigations (PSis), the position sensitivity or duties associated, and the agency authorized to conduct PSis.

Target Audience: DoD civilian, military and contractor personnel

Requirements: A passing score of 75% on the final exam

Privileged User lA Responsibilities:

Description: Developed to be used in conjunction with annual DoD information assurance (lA) awareness training, this course presents the additional IA responsibilities for DoD information system users with access privileges elevated above those of an authorized user. The course identifies key terminology describing elevated user privileges, specific ethical and legal lA responsibilities of a privileged user, and DoD Public Key Infrastructure (PKI) responsibilities of a privileged user. Privileged user general IA responsibilities and restrictions covered in this course include: reporting requirements, restricted and prohibited actions, protecting sensitive information, and the consequences of failure to comply. The portion of the course focusing on PKI responsibilities of privileged users reviews general rules for PKI credential use by privileged users, as well as general configuration guidelines for public key enabling of DoD information systems. The course stresses use of appropriate PKI tokens by privileged users for PKI identification and authentication, in addition to ensuring that the system correctly maps PKI certificates to an account with a set of associated privileges. The training delineates the seven sensitivity levels the DoD has defined for sensitive Unclassified and Secret information. These sensitivity levels, in conjunction with the environments from which users may access the information, are used to determine acceptable types of authentication credentials based on the strength of the credentials.

Target Audience: Department of Defense (DoD) information system users with access privileges elevated above those of an authorized user and other U.S. Government personnel and contractors within the National Industrial Security Program with privileged access to DoD information systems.

Security Policies, Principles and Programs:

Description: This course is an interactive Web-based course. The course provides an overview of the various policies, principles, programs, governing documents, as well as explores four overarching security disciplines that govern how the Department of Defense (DoD) implements its security programs. Specific areas include an introduction and background lesson and the course defines the role of the Federal Government and DoD security responsibilities.

Target Audience: Civilian, military, and contractor personnel responsible for or involved in the safeguarding and protection of DoD assets.

Identifying and Safeguarding Personally Identifiable Information (PII):

Description: This training starts with an overview of Personally Identifiable Information (PII), and protected health information (PHI), a significant subset of PII, and the significance of each, as well as the laws and policy that govern the maintenance and protection of PII and PHI. The course is designed to prepare DoD and other Federal employees to recognize the importance of PII, to identify what PII is, and why it is important to protect PII. The Federal government requires the collection and maintenance of PII so as to govern efficiently. However, because PII is sensitive, the government must take care to protect PII, as the unauthorized release or abuse of PII could result in potentially grave repercussions for the individual whose PII has been compromised, as well as for the federal entity entrusted with safeguarding the PII. This course explains the responsibilities for safeguarding PII and PHI on both the organizational and individual levels, examines the authorized and unauthorized use and disclosure of PII and PHI, and the organizational and individual penalties for not complying with the policies governing Pll and PHI maintenance and protection. This training is intended for DoD civilians, military members, and contractors using DoD information systems. This course may also be used by other Federal Agencies.

Target Audience: DoD information system users, including military members and other U.S. Government personnel and contractors.

2.4.24 Identity Management

Validates and securely authenticates an identity (human, device, system, or service) requesting use of an IT asset prior to granting access, with the exception of weapons systems. Identity management includes but is not limited to, the use of the CAC, PKI, and biometric technologies.

2.4.25 Digital Signatures

All forms of electronic correspondence requiring either message integrity or non-repudiation are signed digitally using DoD PKI. All forms of electronic correspondence containing an attachment or embedded active content are digitally signed.

2.4.26 Mission Assurance Categories (MAC)

The MAC must be selected based on the importance of the information in the system relative to the achievement of DoN goals and objectives; particularly the war fighter mission, not the cost of IA factors associated with a particular MAC. There are three Mission Assurance Categories, MAC I, MAC II, and MAC III as described below.

MAC I systems handle information vital to the operational readiness or effectiveness of deployed or contingency forces. The loss of MAC I data would cause severe damage to the successful completion of DoD missions. Therefore, MAC I systems are required to maintain the highest level of integrity and availability, along with the most precise measures of protection.

MAC II systems handle information important to the support of deployed and contingency forces. The loss of MAC II systems could have a significant negative impact on the success of the mission or operational readiness. The loss of integrity of MAC II data is unacceptable;

therefore MAC II systems must also maintain high levels of integrity. The loss of availability of MAC II data can be tolerated only for a short period of time, so MAC II systems must maintain a medium level of availability. MAC II systems require protective measures above industry best practices to ensure adequate integrity and availability of data.

MAC III systems handle information that is necessary for day-to-day operations, but not directly related to the support of deployed or contingency forces. The loss of MAC III data would not have an immediate impact on the effectiveness of a mission or operational readiness. Since the loss of MAC III data would not have a significant impact in the short term, MAC III systems are required to maintain basic levels of integrity and availability. MAC III systems must be protected by measures considered as industry best practices.

2.4.27 Trusted Associate Sponsorship System (TASS)

TASS allows Affiliated Volunteers (requiring DoD Network access), Contractors, Foreign Affiliates, Non-DoD Civil Service Employees, Non-Federal Agency Civilian Associates, Non-US Non-Appropriated Fund (NAF) Employees, OCONUS Hires, and other Federal Agency Contractors to apply for a Common Access Card (CAC) or other government credential electronically through the Internet. TASS replaces the former Contractor Verification System (CVS) and is the repository of information for Government sponsors and TAs to approve applications for government credentials

2.4.28 Defense Enrollment Eligibility Reporting System (DEERS)

A Worldwide computerized database of uniformed services members, their eligible family members, and others who are eligible for DoD Identification Cards. Provides accurate and timely information for support of DoD identification cards. DEERS obtains and keeps record of the information within the SAAR. It retains authorization of access requests and the information is then automatically synced to TASS.

2.4.29 Identity and Access Management (IdAM)

IdAM is the centralized user admin and/or management of IT systems access rights. The IdAM Strategy builds upon the DoD's existing identity and credential management capabilities; the Common Access Card (CAC) and Public Key Infrastructure (PKI). The CAC and PKI provide the primary enterprise-wide, standardized identity verification and strong cryptographic authentication capabilities and serve as the DoD's implementation of the Federal Personal Identity Verification Card. IdAM seeks to expand and improve existing IdAM infrastructure to better support synchronized and responsive operations across the Joint Information Environment (JIE) by ensuring person and non-person entities can securely access all authorized DoD resources, anywhere, at any time. IdAM can only be as successful as the trustworthiness, completeness, accuracy, and accessibility of the data that is driving the process. In other words, access control is absolutely dependent on the availability and integrity of the data. It is important to note that the data is maintained at a level that is appropriate for the management and use of that data.

IdAM supports the ability to readily look up person entities and non-person entities that have contact data via information systems, while ensuring security safeguards are in place to appropriately limit and/or not expose the contact data for sensitive personnel and populations

2.4.30 System Authorization Access Request (SAAR)

A SAAR is also referred to as DD Form 2875 – a Department of Defense form used to request system authorization access. A SAAR is required for the following: Standard User Accounts, Privileged User Accounts, Modification to User Accounts, Access to Applications and Systems, Logical Moves due to PCS or PCA Orders, Enabling an Account that has been inactive for more than 30 days, and Change of Legal Name.

Digitally signed SAARs are required for the following:

- Authorized User Accounts/Access
- Privileged User Accounts/Access
- Modify User Access
- Deactivation of User Account/Access
- Deletion of User Account
- Access to Applications or Systems
- Logical Moves due to PCS or PCA Orders
- Enabling an account that has be inactive for more than 30 days
- Change of legal name

2.4.31 Certification and Accreditation

The certification and accreditation (C&A) process is an integral part of the life cycle of an IS. The identification of protection measures occurs during system design or development.

The formal C&A occurs after the protection measures have been implemented and any required IS protection documentation has been approved.

Certification validates that the protection measures described in the SSP have been implemented on the system and that the protection measures are functioning properly. Accreditation is the approval by the CSA for the system to process classified information.

2.5 Quality Control

Quality control depends on the implementation and execution of the Continual Service Improvement (CSI) process. CSI confirms that measurements and metrics are in place, milestones attained, the IAM process compliance is high, and IAM meets its business objectives and priorities.

CSI is comprised of seven steps:

1. Identify the strategy for improvement by asking questions
   a) What is the vision?
      What is the mission of Identity and Access Management?
      What is / are the role(s) of IAM?
      What is / are the responsibilities of IAM?
      What else or more must IAM become?
      What role(s) / responsibilities are under satisfied or unsatisfied?

   b) Where are we now?

How is IAM currently fulfilling its mission?
What is the delta between desired customer satisfaction and actual?
What is the delta between desired performance and actual?
Identify and assess risks?

c) Where do we want to be?
Attain and maintain high efficiency.
Attain and maintain high effectiveness.
Attain and maintain high customer satisfaction
Attain and maintain reputation for integrity, dependability, reliability, responsiveness.
Leverage manpower with processes, technology, and automation.
Identify mission critical systems
Identify highest priority customers (customer hierarchy)

d) How to increase efficiency?
Consistent, repeatable processes
Minimize exceptions, special handling, unnecessary processes, unnecessary actors / participants
Dependable technology
Automation
Mitigate / eliminate risk

e) How to increase effectiveness?
Exercise deliberate speed (time is money, but haste makes waste)
Consistent, reliable, dependable input, processing, output
Mitigate / eliminate risk

f) How to increase customer satisfaction?
Tackle findings from customer surveys
Reliability
Dependability
Consistency
Responsiveness
Speed

g) How do we get there?
Call upon Subject Matter Experts and stakeholders
Investigate via Root Cause Analysis (RCA) or other methodology.
Analyze and prioritize
Compile lessons learned
Review industry best practices
Evaluate tools and technology
Prototype and pilot

h) Did we get there?
Customer surveys
CSI / QA audits
Internal / external assess / appraisals

2. Define what is measured
Total time to process user request
Total time for IAM processing of user request

Total user requests submitted
Total user requests correctly granted / removed
Total user requests correctly denied
Total user requests incorrectly granted / removed
Total user requested incorrectly denied.
Total time to reconcile user requests incorrectly granted / removed or denied
Total time for IAM to reconcile user requests incorrectly granted / removed or denied.

3. Gather data
   Obtained from incidents, problems, events, alerts, audits, surveys, interviews, logs, knowledge management data base

To answer the CSI questions perform baseline assessments, define measurable targets, produce service and process improvements, collect measurement data, and compile metrics.

2.5.1 Metrics, Measurements and Continual Process Improvement

Continual service improvement depends on accurate and timely process measurements and relies upon obtaining, analyzing, and using information that is practical and meaningful to the process at-hand. Measurements of process efficiency and effectiveness enable the USMC to track performance and improve overall end user satisfaction. Process metrics are used as measurements of how well the process is working, whether or not the process is continuing to improve, or where improvements should be made. When evaluating process metrics, the direction of change is more important than the magnitude of the metric.

Effective day-to-day operation and long-term management of the process requires the use of metrics and measurements. Reports need to be defined, executed, and distributed to enable the managing of process-related issues and initiatives. Daily management occurs at the process manager level. Long-term trending analysis and management of significant process activities occurs at the process owner level.

The essential components of any measurement system are Critical Success Factors (CSFs) and Key Performance Indicators (KPIs). Both CSFs and KPIs establish the baseline and mechanisms for tracking performance. CSFs are those important factors that must be done well within the process. KPIs can then be defined and measured against the process to ensure each CSF is met.

Measurement only becomes meaningful when it is possible to measure the actual output or dimensions of a system, function, or process against a standard or desired level; i.e. the request for access must have a turnaround time of 72 hours from beginning to end. This needs to be defined early on and ideally improved over time.

To implement and execute CSI, IAM has to specify Critical Success Factors (CSFs). CSFs are based on the high-level objectives of IAM and are what must happen if an IAM service, process, or activity is to succeed. In order to know what happens and ensure effective day-to-day operation and long-term management, data is collect and measurements are made and the data and measurements are used to generate metrics or Key Performance Indicators (KPIs).

KPIs are metrics that are developed that are appropriate for the maturity level of IAM, the CSFs, and appropriate for the particular circumstances. KPIs are used to help manage IAM services,

processes, or activities. KPIs are used to measure the achievement of CSFs and used to identify improvements. While many metrics collected only the most important are specified as KPIs. KPIs should be selected to ensure that efficiency, effectiveness are managed.

Reports are defined, executed, and distributed to enable the managing of process-related issues and initiatives.

2.5.1.1 Critical Success Factors with Key Performance Indicators

The following CSFs and KPIs can be used to measure the efficiency and effectiveness of the process. Results of the analysis provide input to improvement programs (i.e., continual service improvement).

Table 2-8 describes the metrics that are required to be monitored, measured and analyzed:

Table 2-7: IAM Objectives

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Ensure that the confidentiality, integrity and availability of services are protected in accordance with information security policy.	1	Percentage of incidents that involve inappropriate security access or attempts to access services.
		2	Number of audit findings that discovered incorrect access settings for users that have changed roles or left the organization.
		3	Number of incidents requiring a reset of access rights.
		4	Number of incidents caused by incorrect access settings.
2	Provide appropriate access to services on a timely basis that meets business needs.	5	Percentage of requests for access (service request, RFC, etc.) that were provided within established SLAs and OLAs.
3	Provide timely communications about improper access or abuse of services.	6	Average duration of access-related incidents (from time of discovery to escalation and/or resolution).
4	Requestor must be able to log in and request access	7	Percentage of login failure attempts or access denied.
5	Request must be routed correctly	8	Percentage of Requests that were routed to the appropriate groups for processing
6	Provide appropriate access to services on a timely basis that meets business needs	9	Average time from when the request is submitted until the user is notified that access has been granted for: • Correctly filled out standard user requests • Correctly filled out privileged user requests • Correctly filled out System Requests Percent of Standard User requests which are correctly filled out, for which the time from when the request is submitted until the user is notified that access has

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
			been granted is less than or equal to 72 hours (working hours). Average time from when the privileged request is submitted until the user receives their token. Percent of Privileged User requests, which are correctly filled out, for which the time from when the request is submitted until the user receives the token, is less than or equal to thirty calendar days (This must be completed in 30 calendar days, or the account is disabled).

The following benefits are responsible for collectively tying back to the CSFs and KPIs. However, they may not be a one to one match to any one particular CSF or KPI. The benefits holistically illustrate the positive outcomes of meeting IAM's objectives and goals.

Benefits to associate with CSF/KPIs:

- The ability to verify the identity of a user (the person is who they say they are)
- The ability to verify the identity of the approving person or body
- The ability to verify that a user qualifies for access to a specific service
- The ability to link multiple access rights to an individual user
- The ability to determine the status of the user at any time (e.g. to determine whether they are still employees of the organization when they log onto a system)
- The ability to manage changes to a user's access requirements
- The ability to restrict access rights to unauthorized users
- Shortened, effective, efficient cycle time for processing user requests
- Reduction in errors in granting inappropriate access privileges
- Effective and efficient removal / denial of access
- Providing correct and appropriate access privileges the first time
- Less rework
- Higher security and information assurance
- Reduced risk

3.0 ROLES AND RESPONSIBILITIES

Each process has roles and responsibilities associated with design, development, execution and management of the process. A role within a process is defined as a set of responsibilities.

Ownership (i.e., accountability): The process owner will serve as the authoritative process point of contact for any higher headquarters (DON or DOD) or adjacent organization engagement or coordination. The process owner will provide oversight of the Identity and Access Management process and ensure IAM is executed throughout the classified and unclassified MCIE. The Process Owner will coordinate regularly scheduled process review boards to evaluate the business value provided by IAM and to discuss recommended enhancements to the process. This team will use this review to evaluate and improve the Critical Success Factors and the Key Performance Indicators that are utilized to measure the success of the IAM Process. Process specific metrics will be developed and monitored to ensure that the KPIs are realistic, measurable and relevant to support the IAM process.

The process owner will appoint an Enterprise level process manager to support the IAM process.

Management (i.e., responsibility) of the IAM process may be shared. A single Enterprise IAM Process Manager exists at the MCNOSC and Regional IAM Process Managers are located at the RNOSC or at the MITSCs depending on regional staffing capabilities. The RNOSC is responsible for Situational Awareness (SA) to the Marine Corps Forces G6 in addition to responsibilities outlined in the Marine Corps Information Environment Concept of Employment. There can also be instances where a single person is responsible for multiple roles. Factors such as Area of Responsibility (AOR), size of user base and size of the process support team dictate exactly which roles require a dedicated person(s) and the total number of people performing each role.

The process manager provides direct support to the process owner by daily operational management of the IAM process. Process Managers report deviations in the processes and recommend corrective action to the respective process owner.

Figure 3-1: Identity and Access Management Roles depicts all the *critical* roles.

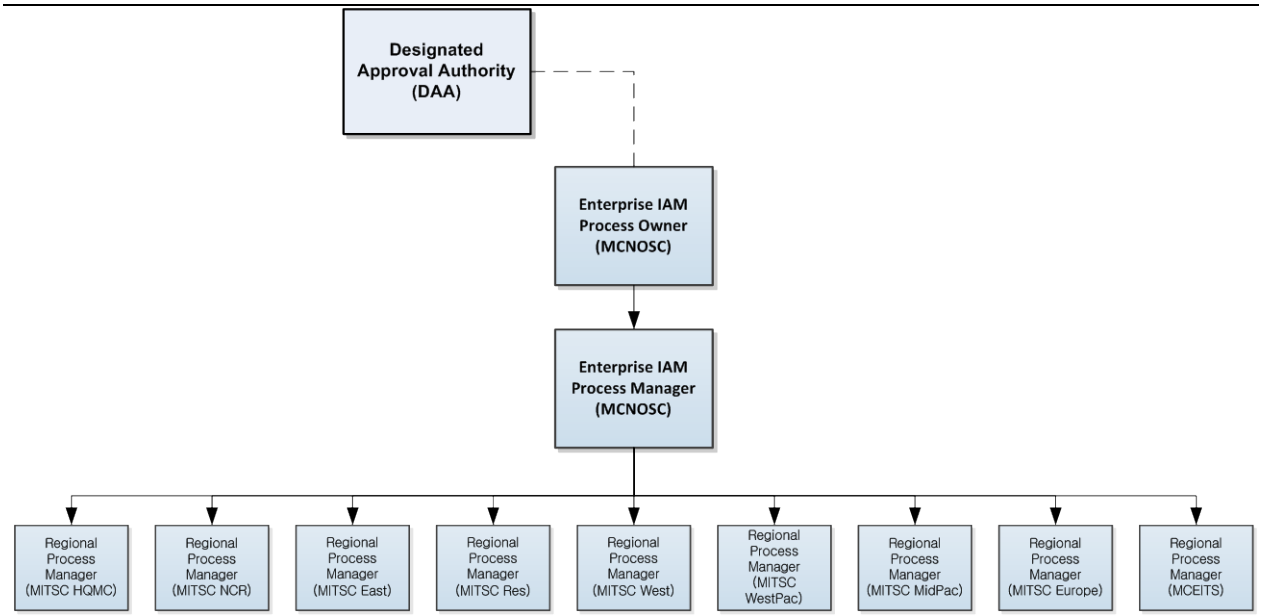


Figure 3-1: Identity and Access Management Roles

Table 3-1 describes roles and responsibilities of Identity and Access Management roles:

Table 3-1: Process Defined Roles and Responsibilities

Process Role Description	Responsibilities
Enterprise IAM Process Owner	
The Process Owner owns the process and the supporting documentation for the process. The primary functions of the Process Owner are oversight and continuous process improvement. To these ends, the Process Owner oversees the process, ensuring that the process is followed by the organization. When the process isn't being followed or isn't working well, the Process Owner is responsible for identifying and ensuring required actions are taken to correct the situation. In addition, the Process Owner is responsible for the approval of all proposed changes to the process, and development of process improvement plans.	• Reviews and understands all references pertaining to process ownership • Documents and publicizes the process • Establishes and communicates the process roles and responsibilities • Ensures updates to the Process Guide are performed according to the Change Management Process • Defines the KPIs to evaluate the effectiveness and efficiency of the process • Reviews KPIs and takes action required resulting from the analysis. • Assist with and being ultimately responsible for the process design • Ensures the IAM process and tools integrate with other ITSM processes and that requirements for the tools are defined • Ensure the effectiveness and efficiency of the IAM Process and working practices through continuous improvement • Reviews any proposed enhancements to the process • Provides input to the ongoing Service Improvement Plan (SIP) • Addresses any issues with the execution of the process • Ensures all relevant staff have the required training and are aware of their role in the process • Ensures that the process, roles, responsibilities and documentation are regularly reviewed and audited • Interfaces with appropriate organizations to ensure that the process receives the necessary staff resources • Ensures all stakeholders are sufficiently involved in the IAM Process • Ensures tight linkage between the IAM Process and other related processes.

Process Role Description	Responsibilities
	• Ensures organizational adherence to the process. • Designs access request workflows.
Enterprise IAM Process Manager	
The Enterprise IAM Process Manager ensures effective coordination of activities for service quality. The Enterprise IAM Process Manager manages and coordinates all activities necessary to manage granting and revoking access. The Enterprise IAM Process Manager will communicate and coordinate with their regional counterparts (e.g., Regional IAM Process Managers, Service Managers, etc.) when required/beneficial. The Enterprise IAM Process Manager manages the entire IAM process life cycle.	• Works with the Process Owner to plan and coordinate all IAM activities. • Ensures that IAM activities are carried out as required throughout the service lifecycle • Monitors and reports on process performance • Identifies improvement opportunities for inclusion in the CSI register • Works with the CSI Manager and the IAM Process Owner to prioritize improvements in the CSI register • Plan and manage support for IAM tools and process • Coordinates interfaces between IAM and other processes
Regional IAM Process Managers (MITSC, MCEITS, B/P/S)	
The Regional IAM Manager manages and coordinates all activities necessary to manage local IAM responsibilities delegated to them by the IAM Process Owner, within their respective region (MITSC). Regional IAM Process Managers will communicate and coordinate with their counterparts when required/beneficial. Regional IAM Process Managers will work through the Service Owners/Managers to coordinate action required in support of the IAM process. There will be multiple Regional Process Managers.	• Works with the Enterprise IAM Process Manager to plan and coordinate all IAM activities within their AOR. • Ensures that IAM activities are carried out as required throughout the service lifecycle within their AOR. • Monitors and reports on process performance within their AOR. • Identifies improvement opportunities for inclusion in the CSI register to the Enterprise IAM Process Manager. • Works with the CSI Manager and the Enterprise IAM Process Manager to prioritize improvements in the CSI register • Plan and manage support activities for IAM process and training within their AOR.
Requester	
The requester is responsible for completing the required training for the level of access they are requesting). The following personnel have authority to request on behalf of another individual: CTRs, ISCs, Trusted Agents (TAs), and Supervisors. ISCs are located throughout the USMC wherever commands have decided to implement them in accordance with the USMC ISC guidance.	• Completes and signs Access Request • Completes required Information Assurance training • Assures that access rights are managed in accordance with DoD and USMC regulations and guidelines • Informs appropriate authorities of any actual or potential breach of access security
Reporting Analyst	
The Reporting Analyst will work with their respective Regional and/or Enterprise Process Manager in capturing the necessary reports to support the IAM process.	• Provides analytics and reports on information and trending activities as necessary to their respective Regional and/or Enterprise Process Manager(s)

Process Role Description	Responsibilities
Information Systems Coordinators (ISCs)	
The ISC may be the first point of contact for MCEN customers who need IT service support	• Generates trouble ticket records for the customer while interfacing with them. • Tracks and records all associated customer support activity and changes in the status of the trouble ticket record, throughout the lifecycle of the record.
Application Manager	
The Application Manager supports the IAM process throughout the Service Lifecycle	• During service design, supports creation of mechanisms to simplify and control IAM on each service designed • Specify ways in which abuse of rights can be identified and stopped • During service transition, test the service to ensure that access can be granted, controlled and prevented, as designed. • Support investigation of incidents and problems related to IAM
Local Government Supervisor	
The supervisor of the requester will identify the access levels required by the requester.	• Identifies access requirements of requester • Approves access request • Contract officer representative (COR) – (for Contractors)
Local Government Security Officer	
The local Security Officer ensures that the requester has the appropriate security clearance for the access level being requested, and that appropriate IA training has been completed.	• Validates requester security clearance • Validates requester training completion • Approves access request
Local Government IAO/IAM	
The local IAO/IAM ensures that the requester has the appropriate security clearance for the access level being requested, and that appropriate IA training has been completed.	• Validates requesters need to know • Validates requester security clearance • Validates requester training completion • Approves access request • Retains completed DD Form 2875/2875A SAAR
Customer Technical Representatives (CTRs)	
The CTR is responsible for creation of the Service Request, and ensuring that all requirement documentation is attached to the request	• Ensures appropriate documentation is included in the request • Approves Service Request for routing
Local Help Desk Technician (MITSC or G6)	
The Local help desk technician will act as the Information Owner for the access request. They will route requests for access to the appropriate approvers. They will also support the user with troubleshooting access issues.	• Is responsible for the quality of the content of the service request • Provides troubleshooting support to the requester in gaining access • Is the “Information Owner” for access requests covering authorized users and regional privileged users within their AOR. • Creates authorized user and level 2 and 3 privileged user accounts in response to Service requests within their AOR. • Communicates with Requester to gain access to account • Requests additional approval for regional privileged user account requests • Supports their region with provisioning Standard User and Regional Privileged Accounts.
Defensive Cyber Operations Section (DCOS) MCNOSC	
The DCOS monitors enterprise privileged user accounts	• Monitor and track all privileged account access throughout the MCEN. • Identify misuse or malicious activity of privileged accounts.

Process Role Description	Responsibilities
Enterprise Services MCNOSC	
Enterprise Services creates enterprise privileged user accounts	• Creates enterprise privileged user account • Communicates with requester to provide access to the account
PKI RA-OPS MCNOSC	
PKI RA-OPS is responsible for the creation of alternate tokens for privileged user accounts	• On request, provides alternate tokens
Security MCNOSC	
Security conforms that all requirements are met for all enterprise privileged account requests.	• Confirms security requirements are met
Accounts Management	
Enterprise and Regional Entities that are responsible for managing accounts Accounts Management personnel should be identified per system. These individuals will be the touch labor support for the IAMs.	• Will review bi-monthly account and access reports • Submit SRQs to correct discrepancies identified by the bi-monthly account and access report • Will perform semiannual audits on all accounts within their AOR to ensure account information, access, IA Training, and SAARs are current and accurate • Work with Regional IAM Process Mgr on all access related activities • Provide recommendations for IAM Process Improvement to the Regional IAM Process Mgr • Submits all Service Requests for User Accounts within their AOR into the Enterprise Ticketing System • Edits User Account Attributes within AD & GAL updates • Moves User Accounts, Home Folders, & Mailboxes • Creates or Changing Distribution Groups and Security Groups • Enables/Disables User Accounts • Resets/Changes Passwords • Deletes User Accounts
Information Owner	
The functional appointee responsible for approving access to the system being requested.	• Receives, reviews, and validates access request is properly filled out • Determines validity of request for approval • Tracks the request through its lifecycle • Keeps a copy of the completed SAAR (physical and/or in the database) • MCNOSC signs as the Information Owner for Level 4 & 5 Privileged User Accounts • MITSCs sign as Information Owner for Level 2 & 3 Privileged and Authorized User Accounts

3.1 Responsibilities

The processes span organizational boundaries; therefore, procedures and work instructions within the process need to be mapped to roles within the process. These roles are then mapped to job functions, IT staff and departments. The process owner is accountable for ensuring process interaction by implementing systems that allow smooth process flow.

The Responsible, Accountable, Support, Consulted, and Informed, (RASCI) model is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks.

Responsible — Completes the process or activity; responsible for action/implementation. The degree of responsibility is determined by the individual with the "A."

Accountable — Approves or disapproves the process or activity. Individual who is ultimately answerable for the task or a decision regarding the task. Typically, the Process Owner is Accountable for a process, and there must be only one Accountable specified for each task or deliverable.

Support **—** Resources allocated to Responsible, and will assist in completing the task.

Consulted — Gives needed input about the process or activity. Prior to final decision or action, these subject matter experts or stakeholders are consulted.

Informed — Needs to be informed after a decision or action is taken. May be required to take action as a result of the outcome. This is a one-way communication.

Table 3-2 establishes process role responsibilities for high-level process activities as they relate to Enterprise and Regional process roles. Process roles transcend organizational boundaries; therefore a role based RASCI chart ensures proper assignment of responsibilities to individuals.

Table 3-2: RASCI Model for IAM by Process Role

IAM Sub-Processes	DAA (C4-CY)	Process Owner	Enterprise Process Manager	Regional Process Managers	Requestor	Reporting Analyst	Local Government Security Office	Local Government Supervisor	Local Government ISSO/ISSM	Service Desk	Accounts Management
Verification	C	A	R	S, R	R,S	I	R	R	R	I	R
Request Access	C	A	R	S, R	R	I	S,C	R	R	S	I
Change Access	C	A	R	S, R	S	I	I	I	C	S	R
Providing Rights	C	A	R	S, R	I	I	I	I	C	S	R
Monitoring Identity Status	C	A	R	S, R	I	R,S	I	I	R	S	S,R
Log and Track	C	A	R	S, R	R	S	I	I	I	S	S,R

Legend:
Responsible (R) – Completes the process or activity
Accountable (A) – Authority to approve or disapprove the process or activity
Support (S) – Assists in execution of process or activity
Consulted (C) – Experts who provide input
Informed (I) – Notified of activities

Note: Any role that is designated as Responsible, Accountable, Support, or Consulted is not additionally designated as Informed because being designated as Responsible, Accountable, Support, or Consulted already implies being in an Informed status.
Note: Only one role can be accountable for each sub-process.

4.0 SUB-PROCESSES

The USMC ITSM IAM process consists of 5 sub-processes. The following is a description of the Identity and Access Management sub-processes.

4.1 Verification (sub-process 1.0)

Verification includes validating the identity of an entity against an issued credential and / or available data within IdAM. The successful authentication of an entity allows for the next step of determining authorized access to a DoD resource. Authorization is the manual or automated step, governed by the resource owner, where the access control decision is based on the entity's data and relevant access policies. IdAM supports access accountability by binding an entity's identity to authentication and authorization decisions associated with a resource. The Verification sub process balances the "need to know" with the "need to request." IdAM ensures complete, trusted, and accurate IdAM data is readily accessible to resource owners to support access control decisions. IdAM also has the ability to synchronize and make available accurate, enterprise-wide contact data so that authorized entities are able to easily look up entities that have contact data. The prerequisite for this process is that the user has a CAC.

The following workflow (Figure 4-1) depicts the Verification sub-process.

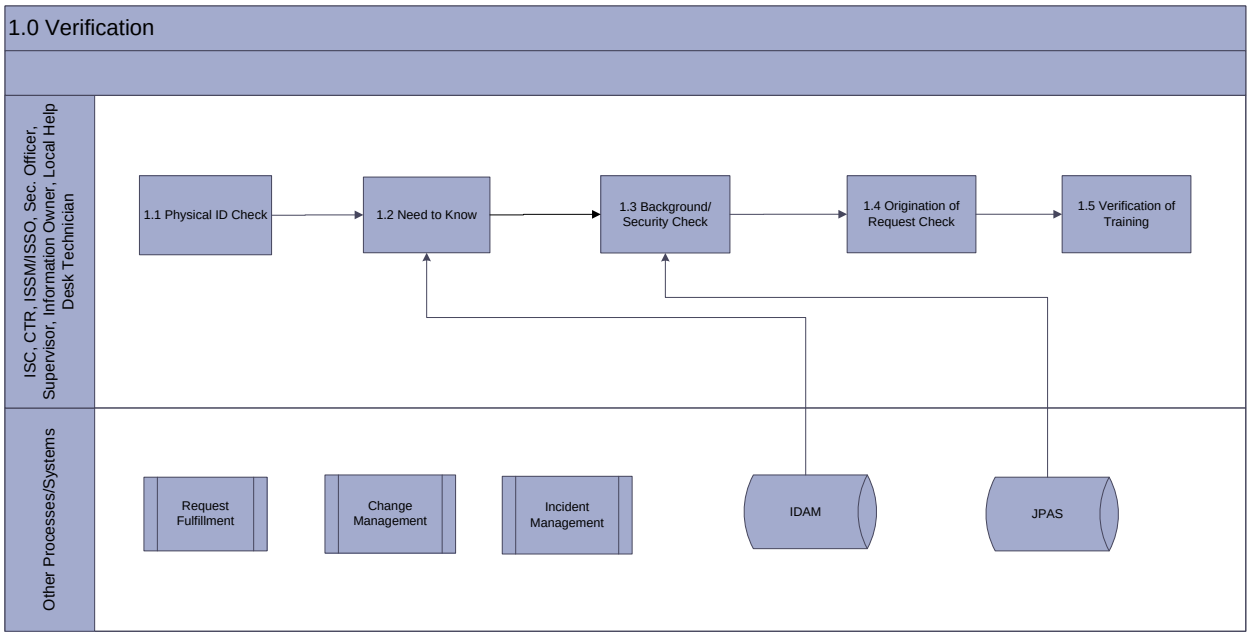


Figure 4-1: Verification Sub-Process

Table 4-1 describes the activities in the Verification sub-process.

Table 4-1: Verification Sub-Process Descriptions

1.0 Verification		
Number	**Process Activity**	**Description**
1	Physical ID Check	Verify physical identification of the individual requesting access. Physical ID Check covers various legal forms of IDs issued for Military personnel, DoD Civilians, and Contractors (Driver's license, CAC Card, government issued identification, etc.).
2	Need to Know	Validate that the individual has a need to know. Need to know is already established based on the individual's role. This information is available through IDAM.
3	Background/Security Check	Check individual's security clearance, background check, and criminal background in JPAS.
4	Origination of Request Check	Validate the origination of the request (i.e. CTR, Manager, ISC, Watch Officer, etc.).
5	Verification of Training	Verify training requirements are met for standard or privileged account.

4.2 Create New Account(s) (sub-process 2.0)

a. Define Access Type
   i. Active Directory (AD)
      1. AD Infrastructure
      2. AD/LDAP Integrated Applications
      3. Data Store
   ii. Transport Services (Network Device)
   iii. System Application
      1. Website
      2. Database
      3. Software
      4. Middleware
      5. Data Store (not AD/LDAP integrated)

The following workflow (Figure 4-2) depicts the Create New Account(s) sub-process. For additional representation of detailed workflow pertaining to Create New Account(s), see Appendix C – N of this document.

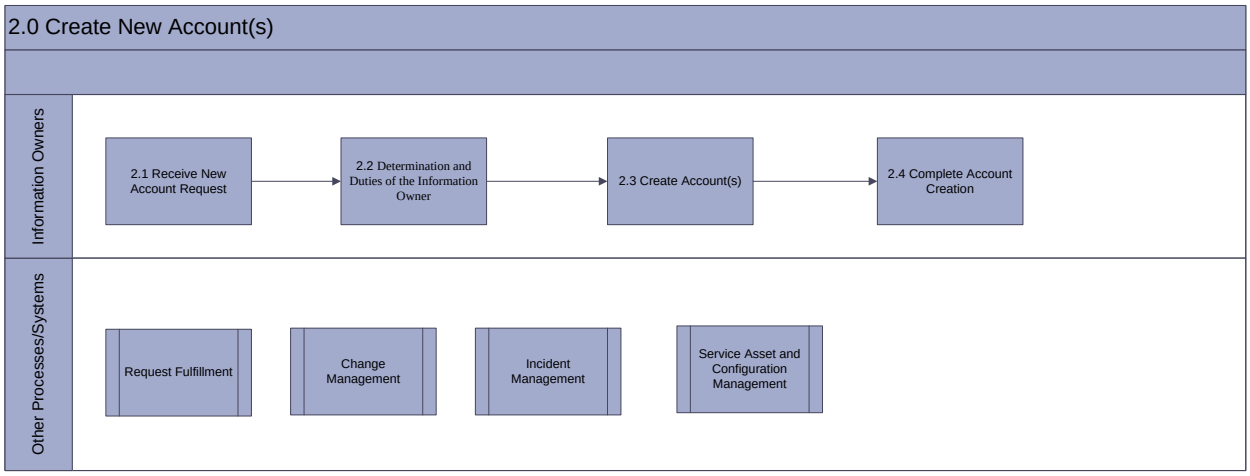


Figure 4-2: Create New Account(s) Sub-Process

Table 4-2 describes the activities in the Create New Account(s) sub-process.

Table 4-2: Create New Account(s) Sub-Process Descriptions

2.0 Create New Account(s)		
Number	**Process Activity**	**Description**
1.	Receive New Account Request	Receive the new account request. Based on the user's AOR, determine who owns what we want access to (MCNOSC, MITSC, B/P/S, Tenant Support Commands, Application Owner, Program of Record (POR), etc.).
2	Determination and Duties of the Information Owner	Review request, validate it was properly filled out by all parties responsible for signature and/or approval, make a decision on whether the request is valid and eligible to proceed to access provisioning. They track the access throughout the lifecycle of the access request (keep a physical copy of the SAAR). The completed SAAR is later returned to the IO when the access request has been created/completed (Once the SAAR is completed, transfers to SACM to become a CI within the CMDB – tracked, monitored, related to other CIs, to support reporting of access controls). Determine the type of account(s) being created. Determine if the account being created is a Privileged or Authorized account. If privileged account, determine at what level.
3	Create Account(s)	Determine the Domain/Network of the account(s) being created. If requested level of access is 4 and/or above, the account creation request comes to the MCNOSC. For DoD Civilians and Contractors, determine if the account creation requires a new Active Directory entry, mailbox, or home folder. SOPs and other documented procedures may exist and vary according to the user's AOR.
4	Complete Account Creation	Complete account creation after following the appropriate SAAR instructions. For Military personnel, logical moves are facilitated through Request Fulfillment.

4.3 Change Access (sub-process 3.0)

Change Access entails a multitude of changes in permission levels, accounts, access, and rights. Change Access also includes disabling and deleting accounts. Deleting an account in its entirety occurs after the account has been disabled. Logical moves entail stripping the access of an account and adding new access. The deactivation of an account is more complex and long term. All rights and permissions are stripped and put into holding OU. The rights and permissions levels should be kept track of prior to stripping the account.

1. Active Directory
   A. Delete Account
   B. Disable Account
   C. Move Account
   D. Change Access Control
   E. Enable Accounts
   F. Change Passwords
   G. Unlock Account
   H. Reset Password

2. Transport
   A. Delete Account
   B. Disable Account
   C. Move Account
   D. Change Access Control
   E. Enable Accounts
   F. Change Passwords
   G. Unlock Account
   H. Reset Password

3. System Application
   A. Delete Account
   B. Disable Account
   C. Move Account
   D. Change Access Control
   E. Enable Accounts
   F. Change Passwords
   G. Unlock Account
   H. Reset Password

The following workflow (Figure 4-3) depicts the Change Access sub-process. For additional representation of detailed workflow pertaining to Change Access, see Appendix C – N of this document.

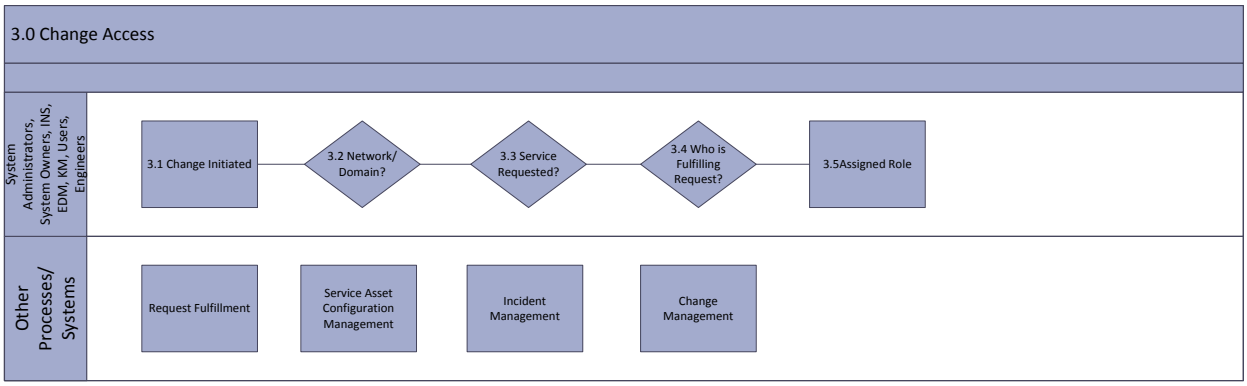


Figure 4-3: Change Access Sub-Process

Table 4-3 describes the activities in the Change Access sub-process.

Table 4-3: Change Access Sub-Process Descriptions

3.0 Change Access		
Number	**Process Activity**	**Description**
1	Change Initiated	The Change Access request is initiated through Request Fulfillment (users), standard changes, or through the Change Management process (Engineering).
2	Network/Domain	A determination is made on whether the service being requested is associated with Active Directory, Transport Services, or a System Application.
3	Service Requested	A determination is made on what type of service is being requested to include: deleting, disabling, moving, changing access controls, enabling, changing passwords, resetting passwords, and unlocking accounts.
4	Who is Fulfilling Request	A determination is made on who is fulfilling the request to include System Owners and Administrators at the MITSCs or MCNOSC. For Active Directory the fulfillment would occur with the EDM team (MCNOSC), for SharePoint Knowledge Management (MCNOSC), and for Transport Services the INS team (MCNOSC).
5	Assigned Role	There are multiple control groups that are setup. Role based permissions will be assigned as applicable.

4.4 Check and Monitor Identity Status (sub-process 4.0)

Check and Monitor Identity Status enables the appropriate DoD security elements to accurately monitor and detect anomalous behavior and support the investigation of those who abuse authorized access to DoD resources. A semi-annual audit cycle will be initiated to ensure that no rogue accounts are on the devices. Spot checking audits will be conducted as accounts are created, modified or deleted. An audit cycle will be initiated in conjunction with all password changes. All system passwords will be verified by an individual other than the one whom made

the modification. Monitoring access activity and enforcing accountable access behavior is the responsibility of operational and security organizations such as the Cyber Command, IT service providers, and information personnel.

Remedy users with the appropriate level of access and need to know have the ability to search for tickets (perform basic or advanced searches), run an existing report, create a new custom report, export reports in PDF, Excel, with Hyperlink support, open Web or legacy AR System Reports, save reports, query reports by date range, share reports with others by post authorization from NETCOP or the Service Desk team that is servicing them, create summary report pages, schedule reports on a predefined timeline or individuals and groups, and delete reports that were created by themselves but no longer needed.

The following list of reports are out of the box reports within Remedy, or have the ability to be created as custom reports for future reporting needs. The preliminary list serves as an example to show future capabilities that the USMC would leverage in support of checking and monitoring, auditing, gathering metrics, and running reports in support of an effective and efficient USMC Enterprise Identity and Access Management process. The below is a list of reports to include but not limited to:

- Number of requests for access (Service Request, RFC, etc.) by reason or region or etc.
- Instances of access granted, by service, by reason or region or etc.
- Instances of access granted by department or individual granting rights
- Number of incidents requiring a reset of access rights by reason or region or etc.
- Number of incidents caused by incorrect access settings by reason or region or etc.
- Number of access denied by reason or region or etc.
- Number of malicious attempts by reason or region or etc.
- Average time from receipt of request to resolution
- Audit for user access to SAAR (every 11 months) based on attributes that identify and track all applications associated with the SAAR
- Weekly reports to establish last logon
- Semi-annual validation of functional mailboxes based on need. Contact the owner (mandatory) to ensure the mailbox in question is still a valid mailbox.
- Number of accounts disabled that are re-enabled within a 60 day timeframe. This shows the volume of accounts and investigation into why they were disabled and enabled so quickly

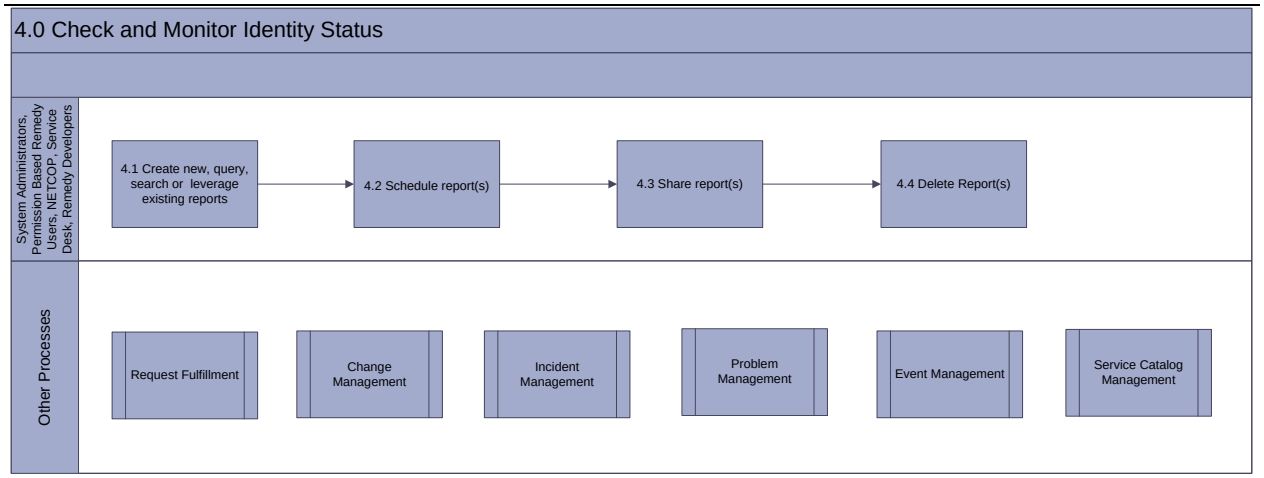


Figure 4-4: Check and Monitor Identity Status Sub-Process

Table 4-4 describes the activities in the Check and Monitor Identity Status sub-process.

Table 4-4: Check and Monitor Identity Status Sub-Process Descriptions

4.0 Check and Monitor Identity Status		
Number	**Process Activity**	**Description**
1	Create new, query, search or leverage existing reports	Create a new custom or out of the box report, leverage an existing report, search (basic or advanced), or query reports within the tool.
2	Schedule report(s)	Schedule reports (daily, weekly, monthly, etc.) with predefined dates and times.
3	Share report(s)	Share report(s) with other stakeholders and/or groups with a need to know post authorization from NETCOP or the Service Desk team that is servicing them.
4	Delete Report(s)	Delete report(s) as needed. A report can only be deleted if you are the original owner/creator of the report.

4.5 Log and Track (sub-process 5.0)

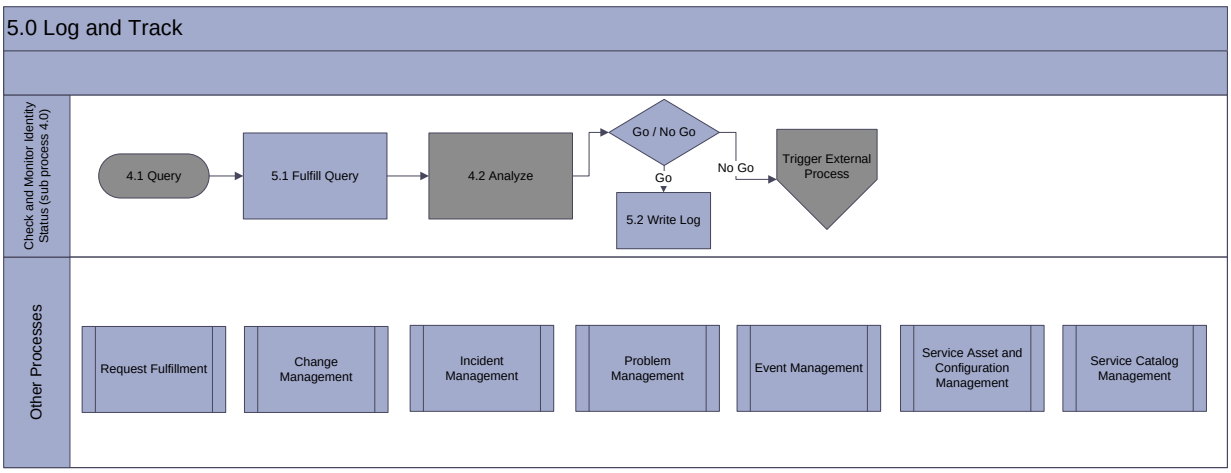


Figure 4-5: Log and Track Sub-Process

Table 4-5 describes the activities in the Log and Track sub-process.

Table 4-5: Log and Track Sub-Process Descriptions

5.0 Log and Track		
Number	**Process Activity**	**Description**
1	Query (4.1)	A query is initiated through the Check and Monitor Identity Status sub process 4.0
2	Fulfill Query (5.1)	The query is fulfilled though the Log and Track sub process
3	Analyze (4.2)	The query is analyzed in the Check and Monitor Identity Status sub process 4.0
4	Go / No Go Decision	A Go / No Go decision is determined
5	Write Log (5.2)	Log entry is captured in the event of a 'Go' decision
6	Trigger External Process (Off-page reference)	An external process or various external processes are triggered based on the unique scenario if a 'No Go' decision is made.

APPENDIX A — ACRONYMS

The official list of E-ITSM acronyms can be found on the Enterprise Information Technology Service Management site (https://eis.usmc.mil/sites/irm/ITSM/default.aspx). The link to the document is referenced below:

https://eis.usmc.mil/sites/irm/ITSM/Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Firm%2FITSM%2FDocuments%2FE%2DITSM%20Acronym%20List&FolderCTID=0x0120001918760B7D35A5478C0474985E3ACBCD&View={9CD820B3-EF85-4D2C-BD0C-A255AEE9E40D}

APPENDIX B — GLOSSARY

Term	Definition
Access accountability	Enhances the monitoring of authentication and authorization decisions to DoD resources to ensure non-repudiation and mitigate the abuse of authorized access.
Access control	The process of granting or denying specific requests to: obtain or use Controlled information and related information processing services; or enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances). A function or a system that restricts access only to authorized persons (DoD Security Lexicon). The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances) (Committee on National Security Systems Instruction 4009, FIPS 201).
Access Management	The management and control of the ways in which entities are granted or denied access to the resources of an organization and are authorized to perform a specific action(s) within a given resource.
Anticipated User	An anticipated user is an entity whose need to access a specific resource is pre-defined and established by the resource owner prior to the entity seeking access (e.g., the user has an account or is on an access control list for the resource the user is seeking access to).
Attributes	The properties or characteristics that describe, distinguish measure, define, and identify entities (DoDD 8320.03).
Attribute Management	The ability to dynamically create, maintain, disseminate, and revoke attributes (e.g., clearances, citizenship, location, biometrics, group memberships, and work roles), which are assigned and bound to subjects
Asset Management	Asset Management is the process responsible for tracking and reporting the financial value and ownership of assets throughout their life cycle.
Authenticate	The act of validating that a claimed identity is genuine and based on valid credentials.
Authentication	A process that matches presented information to the established origin of that information (DoD Security Lexicon). The process of validating that a claimed identity is genuine and based on valid credentials (FICAM).
Authoritative Data Source	A recognized or official data production source with a designated mission statement or source/product to publish reliable and accurate.
Authorization	The process of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities (FICAM).
Authorization Attributes	IdAM data elements used to make authorization decisions. Examples include security clearance, citizenship, billet, organizational affiliation, certifications of training or education, and other specific attributes. Authorization attributes can include attributes from other data categories.
Authorization policies	IdAM access rules or criteria that govern routine automated authorization decisions based on the sensitivity of the protected resource.
Authorize	The act of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities.
Change Schedule	A Change Schedule is a document that lists all approved changes and their planned implementation dates.
Common Access Card	A form of DoD identification card.

Term	Definition
Configuration Item	A Configuration Item (CI) is any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System (CMS) and is maintained throughout its life cycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and SLAs.
CI Type	CI Type is a category used to Classify CIs. The CI Type identifies the required attributes and relationships for a configuration record. Common CI Types include: server, document, user, etc.
Configuration Management Database	A Configuration Management Database (CMDB) is a database used to store configuration records throughout their life cycle. The Configuration Management System (CMS) maintains one or more CMDBs and each CMDB stores attributes of CIs and relationships with other CIs.
Configuration Management Plan	Document defining how configuration management will be implemented (including policies and procedures) for a particular acquisition or program. (Source: MIL HDBK-61A)
Configuration Management System	A Configuration Management System (CMS) is a set of tools and databases used to manage an IT service provider's configuration data. The CMS also includes information about incidents, problems, known errors, changes, and releases and may contain data about employees, suppliers, locations, units, customers and users. The CMS includes tools for collecting, storing, managing, updating and presenting data about all CIs and their relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management processes.
Contract Attributes	See contract data.
Contract data	IdAM information that person and non-person entities have and can be used to discover and interact with each other. Examples include name, telephone numbers, physical addresses, email addresses, rank, contact preferences, and organizational affiliations.
Contract Data Lookup	Provides entities with the ability to readily look up accurate and complete contact information for person and non-person entities.
Contracting Officer (KO)	A government official who, in accordance with departmental or agency procedures, has the authority to enter into and administer contracts and make determinations and findings with respect thereto, or any part of such authority.
Contractor	Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.
Contracting Officer Representative (COR)	Individuals appointed by the Contracting Officer (KO) to assist in the technical monitoring or administration of a contract.
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by an entity (FICAM).
Credentialing	he ability to authoritatively bind an object to an identity (and optionally, additional attributes) to a token possessed and controlled by a person or non-person entity.
Credential Management	Includes the sponsorship, enrollment, issuance and revocation of authentication tokens. An authentication token binds a digital identity to a user in the form of a credential such as a public key infrastructure (PKI) certificate or security assertion markup language (SAML) assertion so that the user can present the token as proof of identity.

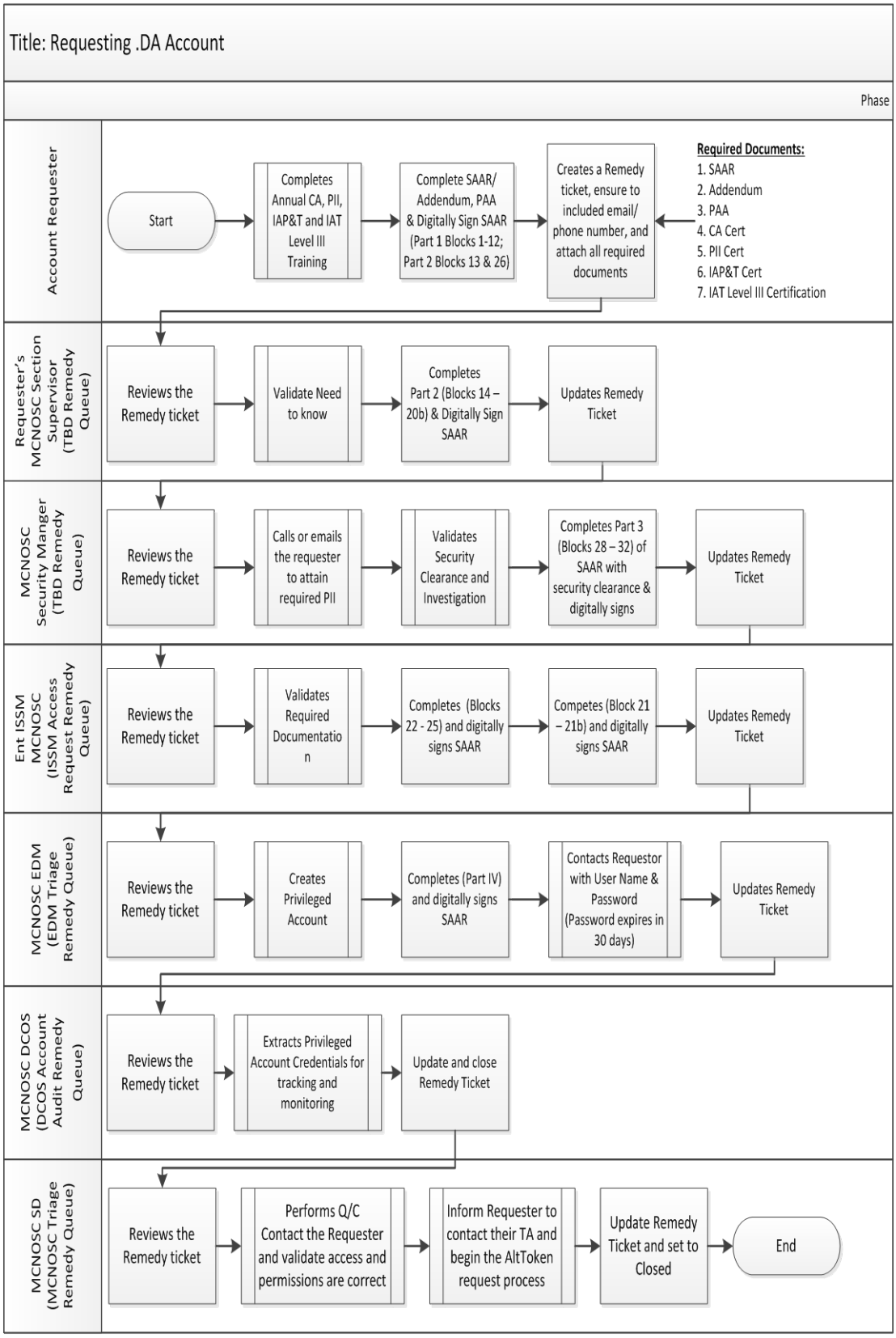
Term	Definition
Credential Strength	The resistance of the identity credential to forgery or fraud, taking into account the strength of the credential technology used (e.g., resistance to copying or brute force attacks), the identity proofing performed prior to issuance of the identity credential, and the protections incorporated into the system issuing and managing the identity credential. Credential strengths are defined for both unclassified and classified environments.
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted.
Digital Identity	The unique set of attribute values (i.e., biographic, biometrics, and contextual characteristics) by which an entity can be distinguished from any other entity in a digital environment.
Digital Identity Management	See Identity Management
Digital Policy	A policy to be enforced by a system that is encoded in such a way that it can be interpreted and enforced by an enterprise system in an automated way, without human intervention.
Digital Policy Management	The ability to dynamically create, disseminate, and maintain hierarchical rule sets to control digital resource management, utilization, and protection. This includes identifying and adjudicating conflicts that may occur among existing and new rule sets due to the hierarchical and dynamic nature of policy. Digital policy may define rules for authentication (trusted authorities, criteria for determining authenticity), authorization (access rules, authorized providers), Quality of Protection (QoP), Quality of Service (QoS), transport connectivity, bandwidth allocation and priority, audit, and computer network defense. Digital Policy Management must protect digital policies, allowing only authorized subjects to create, modify, and delegate management of rules. It assures proper implementation and enforcement of rules through interactions with policy engines and policy enforcement mechanisms and it provision individual aspects of policy decisions to appropriate IA mechanisms.
DoD IT Based Resource	DoD-provided IT devices, systems, applications, and services, and the information and data contained within them.
DoD Resource	A DoD IT-based resource or electronically-protected DoD physical resource such as physical locations, facilities, or other physical objects.
Dynamic Access Control	Automated, data-driven authentication and authorization decisions to DoD resources, anywhere, at any time.
Entity	An independent unit or distinguishable person, place, thing, event, or concept about which information is kept that has distinct features, objects, or attributes associated with it (DoDD 8320.03).
Electronic Physical Access Control System (ePACS)	An automated or electronic system or procedure that supports the controls that manage person or vehicle access to a protected area, by means of authentication and authorization at designated Access Control Points.
Environment	Environment is a subset of the IT infrastructure used for a particular purpose (e.g., live environment, test environment or build environment). It is possible for multiple environments to share a CI (e.g., test and live environments may use different partitions on a single mainframe computer). In the term physical environment, environment can be defined as the accommodation, air conditioning, power system, etc. Environment can be used as a generic term defined as the external conditions that influence or affect something.
Environmental Attributes	Attributes, not specifically about the subject or the resource, but about the current environment at the time of the transaction itself. Environment attributes are critical for fine-grained access control because many of the policies that are enforced on information are conditional on some outside environmental factor rather than just the attributes of the subject requesting access (FICAM).

Term	Definition
Escalation	Escalation is an activity that obtains additional resources when needed to meet service-level targets or customer expectations.
Event	An Event is a piece of data that provides information about one or more system resources. Most events are benign. Some events show a change of state which has significance for the management of a CI or IT service. The term 'event' is also used to define an alert or notification created by any IT service, CI, or monitoring tool. Events typically require IT operations personnel to take actions and often lead to incidents being logged.
Exit and Entry Criteria (Pass/Fail)	These are criteria (defined well in advance and accepted by the stakeholders) defined at authorized points in the Release and Deployment Process to set expectations of acceptable/unacceptable results.
Fitness Attributes	IdAM data elements used to determine suitability of the person or non-person entity requesting access. Examples include attributes indicating known or suspected terrorists, outstanding criminal wants and warrants, debarments, or other mission performance or individual integrity criteria.
Foreign National	Any person who is not a citizen or national of the United States.
Governance	Governance is the process of ensuring policies and strategy are actually implemented and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring, and reporting and taking actions to resolve any issues identified.
Identity	A set of characteristics by which an entity (e.g., human, application, device, service or process) is recognizable and is sufficient to distinguish that entity from every other entity (DoD IdM Strategic Plan).
Identity and Access Management (IdAM)	The policies, processes, architectures, standards, systems, and data that integrate person and non-person entity digital identity management, credentialing, authentication, authorization, and access management.
Identity and Access Management (IdAM) data	All data required to support or make an access control decision to a DoD resource that may include, but is not limited to, an entity's digital identity attributes (e.g., biographic, biometrics, and contextual) and other distinguishing attributes (e.g., contact data, location, role, etc.), entity credentials, resource attributes, access authorization policies, and local security, command, and environmental conditions (e.g., security level, time, location, etc.).
Identity Management	The combination of technical systems, policies and processes that create, define, govern and synchronize the ownership, utilization and safeguarding of identity information.
Incident	An Incident is an unplanned interruption, degradation or reduction in IT Service quality.
Key Terrain Non-Person Entities	Key Terrain Non-Person Entities are primarily drawn from devices that are accessed by multiple DoD Components and/or DoD Mission Partners that require a DoD medium assurance level of trust, as opposed to devices accessible only by DoD relying parties from a single DoD Component and/or domain. Web servers are Key Terrain devices. Other devices to consider for Key Terrain are domain controllers, Domain Name System servers, and routers. Devices such as workstations, printers, and telephones will not be included under Key Terrain at this time.
Key Performance Indicator	A Key Performance Indicator (KPI) is a metric used to help manage a process, IT service, or activity. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, IT service, or activity. KPIs are selected to ensure that efficiency, effectiveness, and cost-effectiveness are all managed.
Logical Access Control System (LACS)	An automated system that controls a person or non-person entity's ability to access an information technology device (e.g., network, application, or device). A LACS requires secure validation of an entity's identity through some pre-determined authentication method which may or may not require the use of a physical token/credential and must have access to IdAM data that indicates an entity's eligibility for access in order to authorize access.

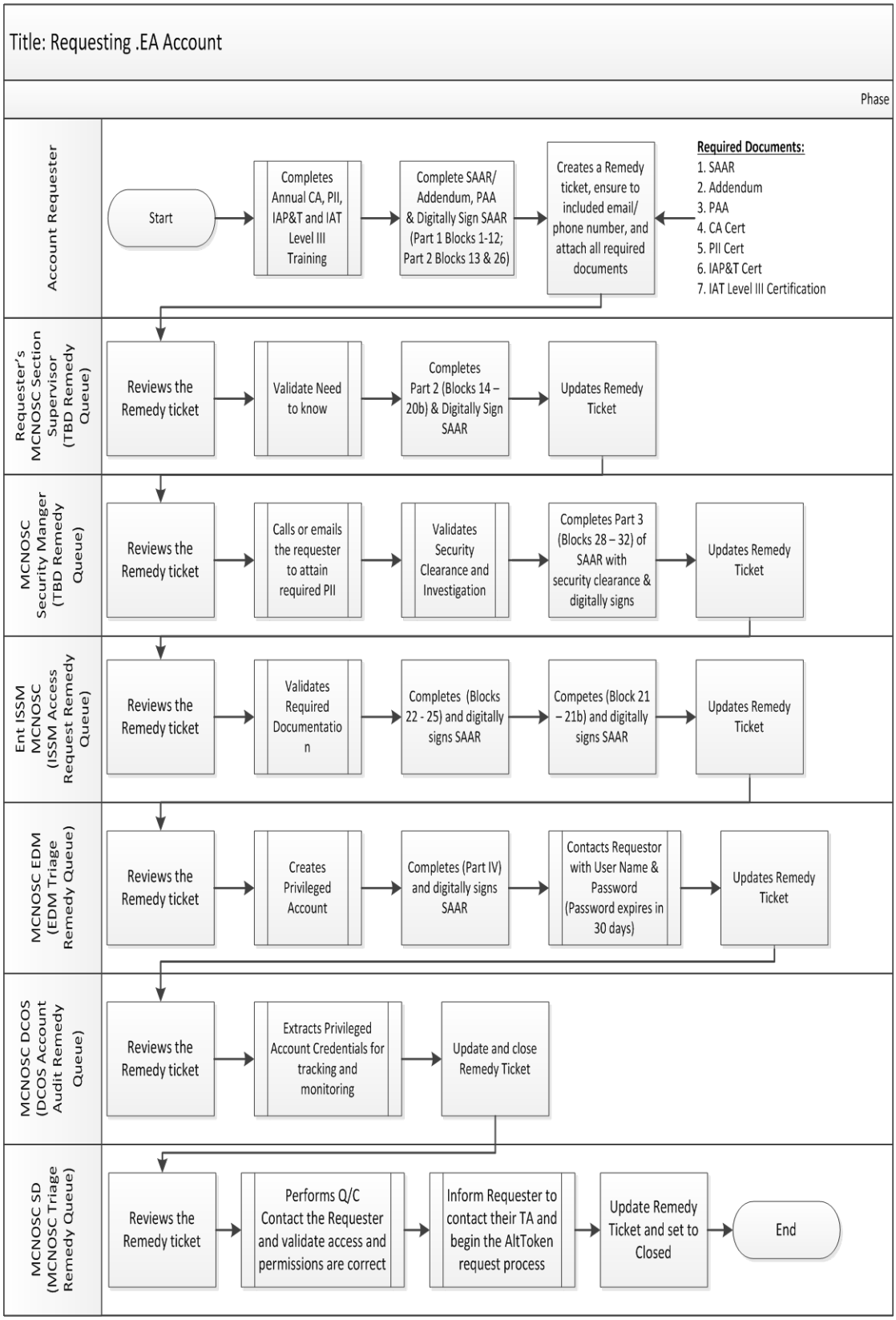
Term	Definition
Manage Access	The act of managing and controlling the ways in which entities are granted or denied access to the resources of an organization, DoD IdAM RA, Operational Activity.
Manage Credentials	The act of sponsoring, enrolling, issuing and revoking authentication tokens.
Manage Digital Identities	See Manage Identities.
Manage Identities	The act of creating, defining, governing and synchronizing the ownership, utilization and safeguarding of identity information.
Manage Identities and Access	The act of managing the integration of person and non-person entity digital identity management, credentialing, authentication, authorization, and access management.
Mission Partners	External partners as defined in the DoD Information Sharing Strategy: Federal, State, local, tribal, coalition partners, foreign governments and security forces, international organizations, non-governmental organizations, and the private sector (DoD Information Sharing Implementation Plan v1.0).
Monitoring	Monitoring is the process of repeated observation of a CI, IT service, or process to detect events and to ensure that the current status is known.
Need to Know	A determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.
Non-Person Entity (NPE)	An entity with a digital identity that is not a person. Examples include an organization, facility (building, conference room, and installation), application, device, network, and unstructured data (documents, imagery, etc.).
Person Entity	A human being with a digital identity.
Personal Identity Verification (PIV)	A physical artifact (e.g., identity card, “smart” card) issued to an 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).
Process	A Process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools, and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities, and work instructions, if needed.
Public Key Infrastructure (PKI)	The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of PK certificates.
Quality Assurance	Quality Assurance (QA) is the process responsible for ensuring the quality of a product and also ensuring it will provide its intended value.
Resource Attributes	Information describing the characteristics of a resource; data or information about the resource; or descriptive information about a resource entity’s data, data activities, systems, and holdings which drive the authorization policies. Examples include, information security markings, need to know metadata, digital policy reference, etc.
Role	A Role refers to a set of connected behaviors or actions that are performed by a person, team, or group in a specific context.
Service Improvement Plan	A Service Improvement Plan (SIP) is a formal plan to implement improvements to a process or IT service.

Term	Definition
Service Level Agreement	A Service-Level Agreement (SLA) is an agreement between an IT service provider and a customer. The SLA describes the IT service; documents service-level targets; and specifies the responsibilities of the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers.
Single Point of Contact	A Single Point of Contact (SPOC) is an agreement used to assign a single, consistent way to communicate within an organization or unit. For example, the Service Desk will be the SPOC for a service provider.
Unanticipated User	An unanticipated user is an entity who is eligible or has a justifiable reason to access a specific resource, however, the resource owner has no previous awareness, nor has made specific allowances for the unanticipated entity to be allowed access (e.g., the user does not have a pre-existing account nor is on an access control list to the resource they are seeking access to).

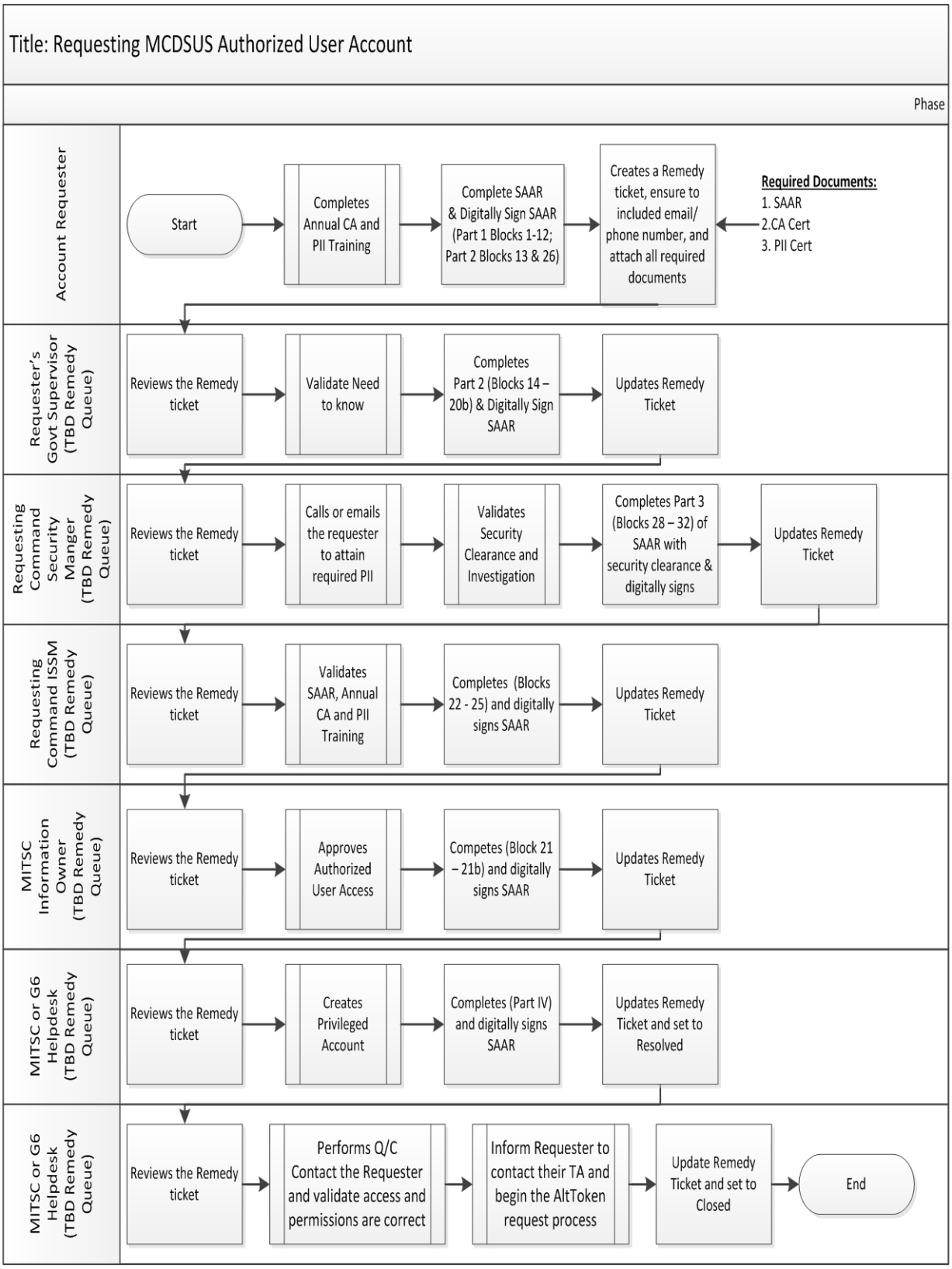
APPENDIX C — REQUESTING .DA ACCOUNT WORKFLOW



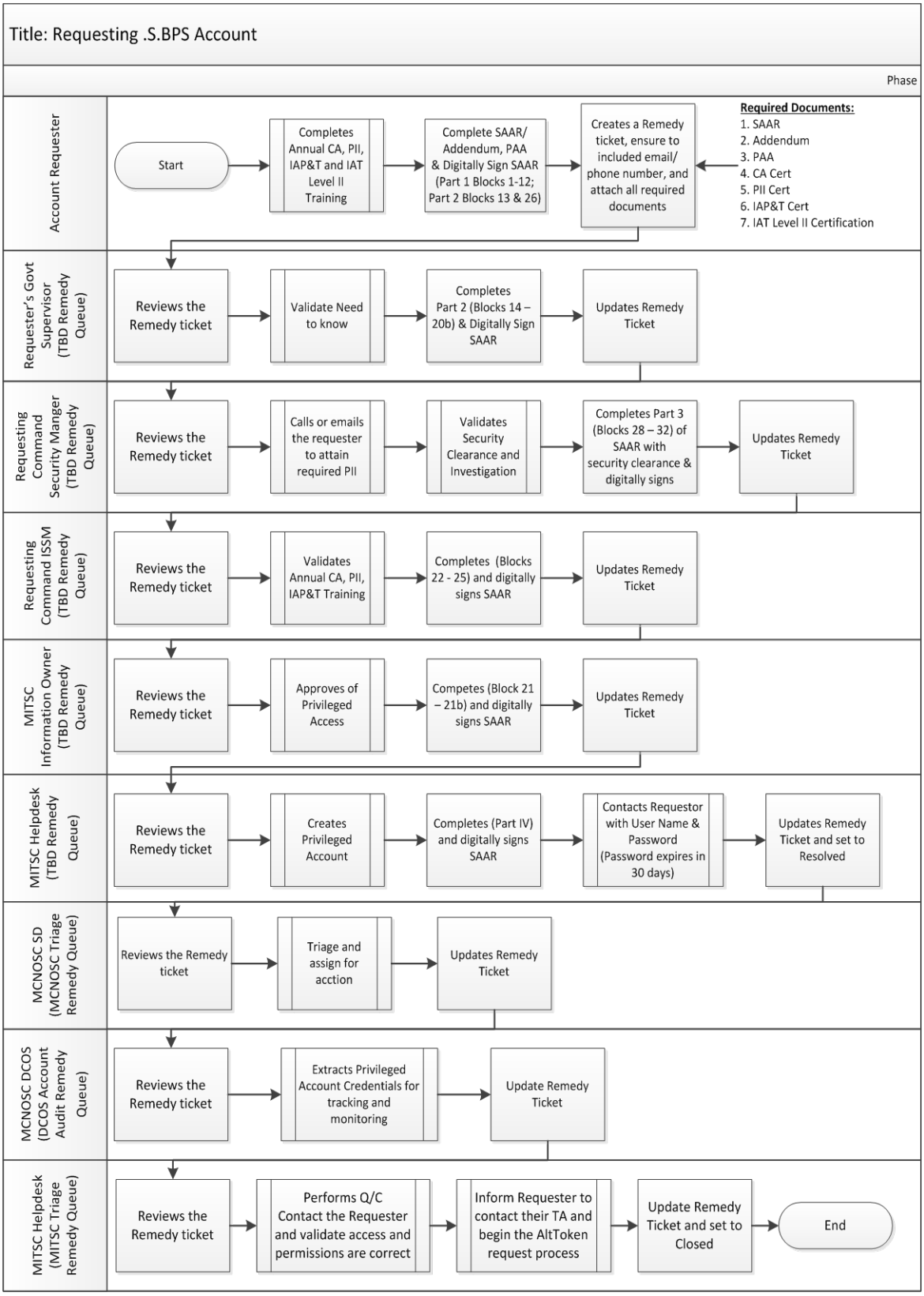
APPENDIX D — REQUESTING .EA ACCOUNT WORKFLOW



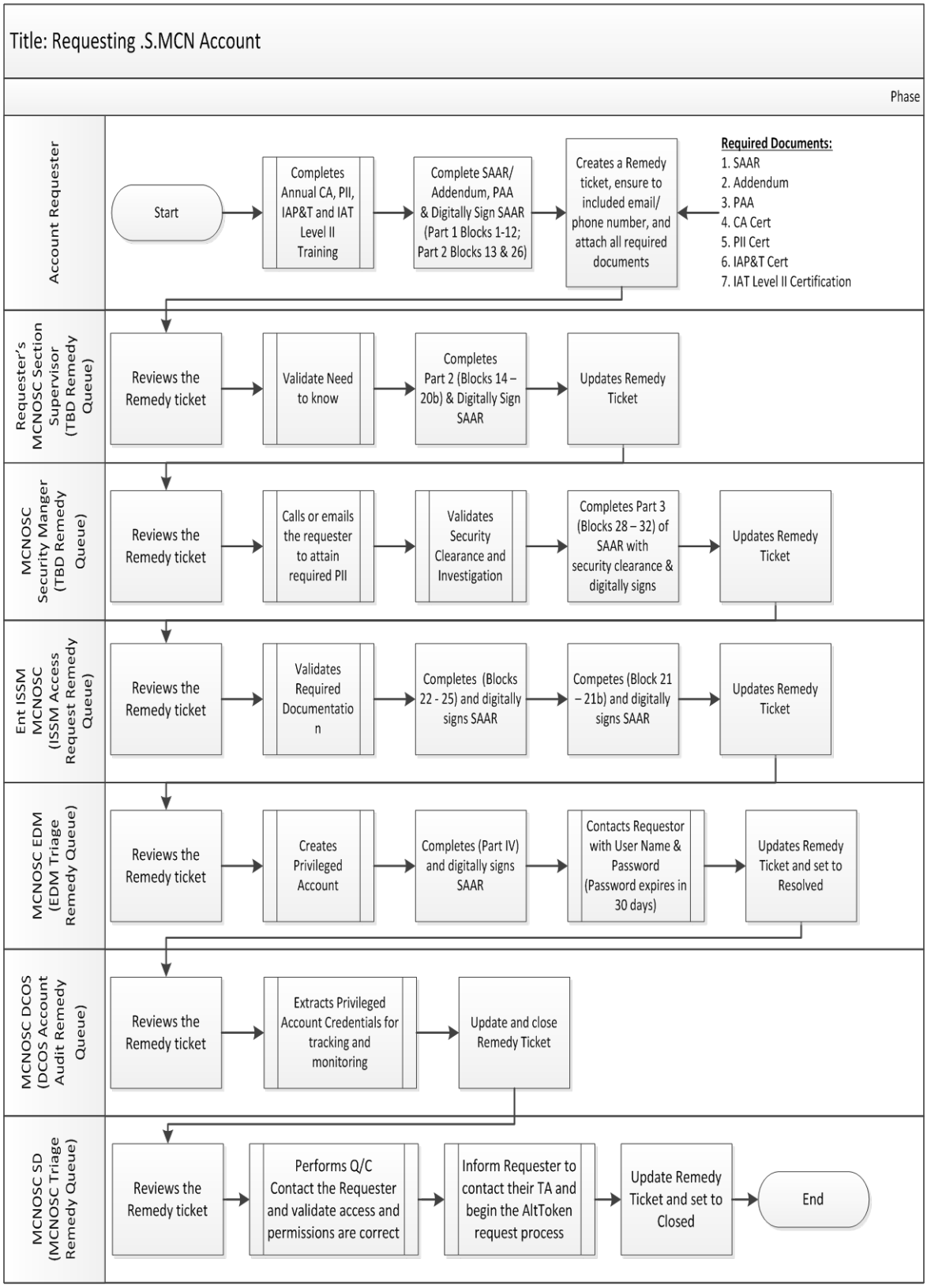
APPENDIX E — REQUESTING MCDSUS AUTHORIZED USER ACCOUNT WORKFLOW



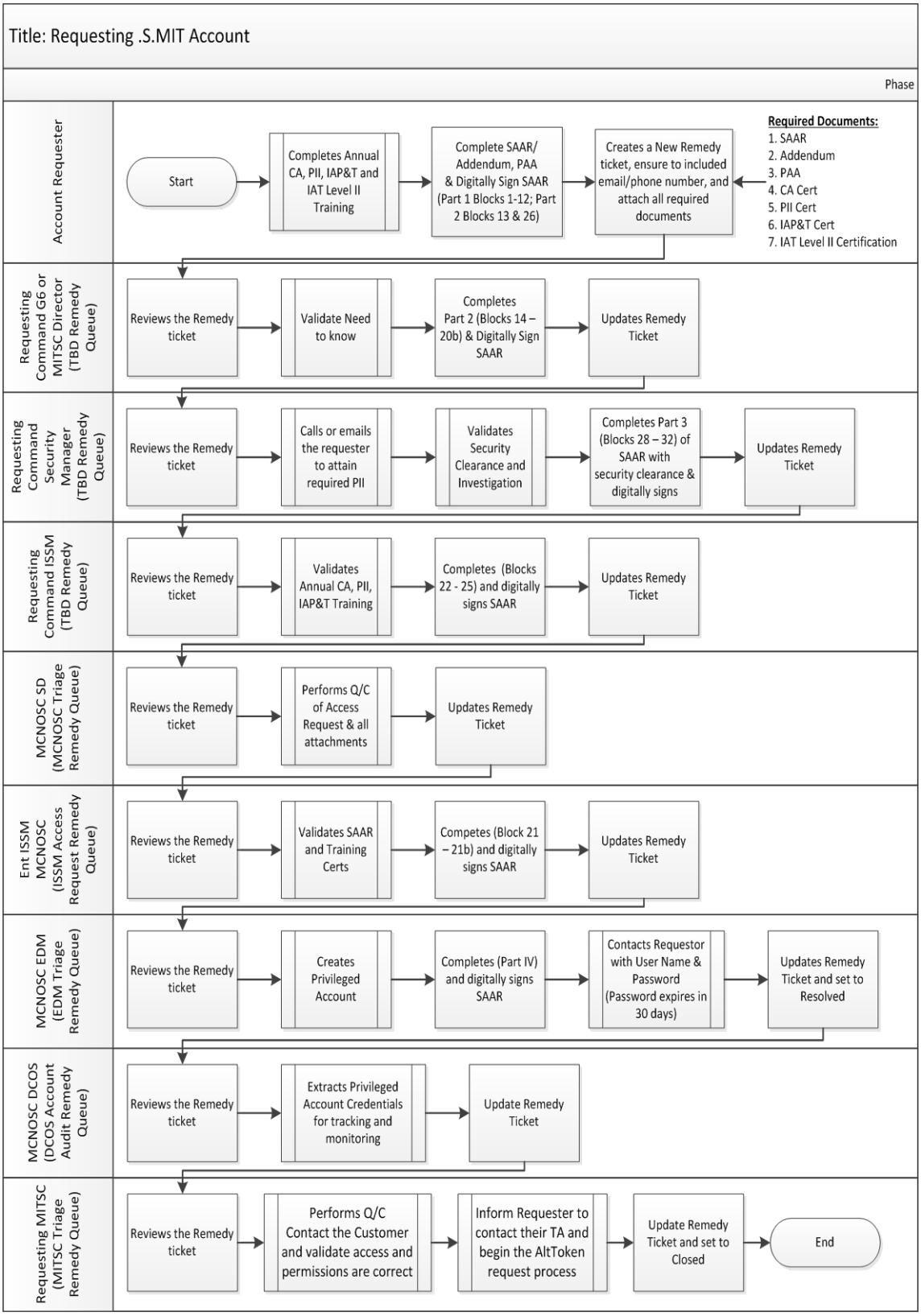
APPENDIX F — REQUESTING .S.BPS ACCOUNT WORKFLOW



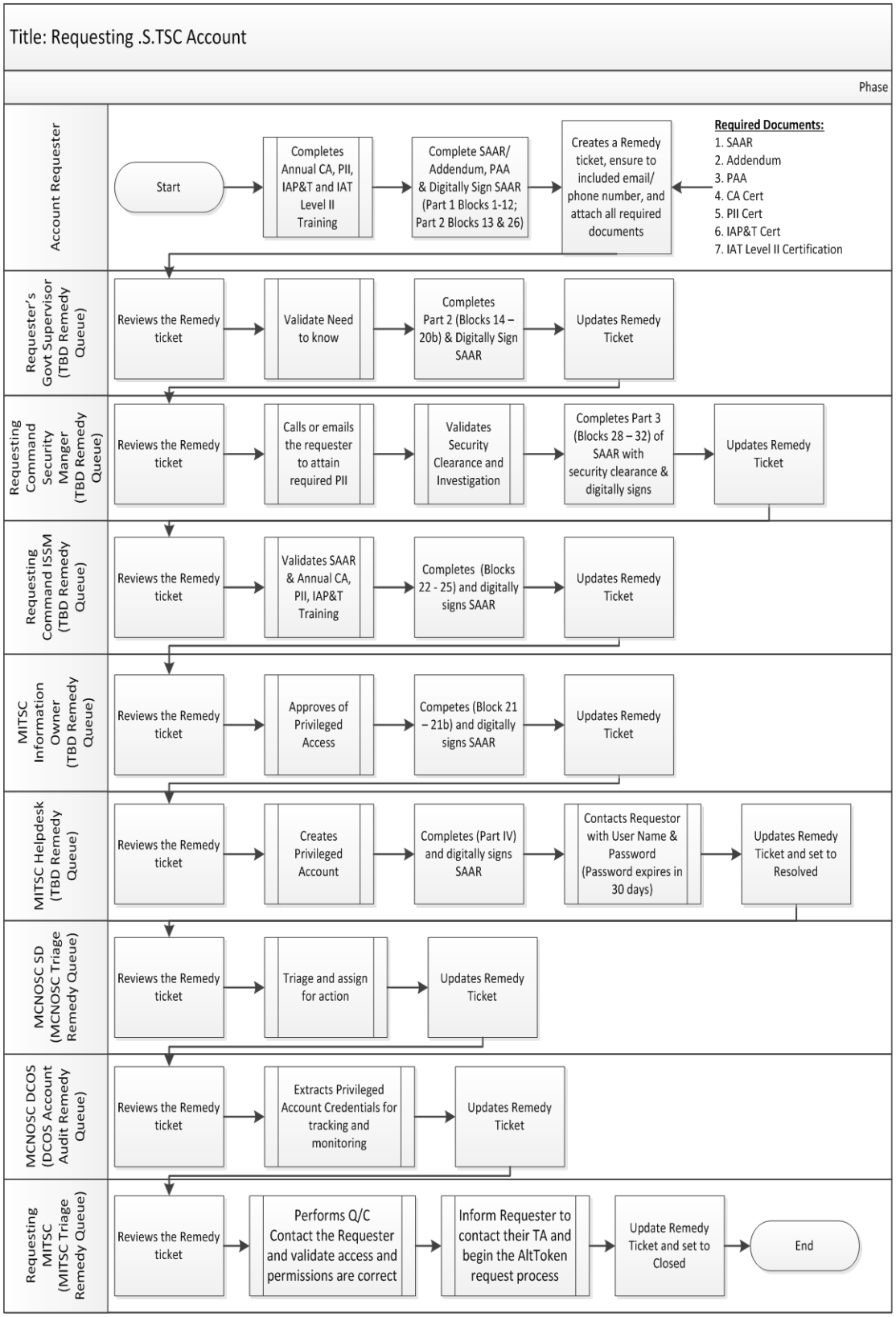
APPENDIX G — REQUESTING .S.MCN ACCOUNT WORKFLOW



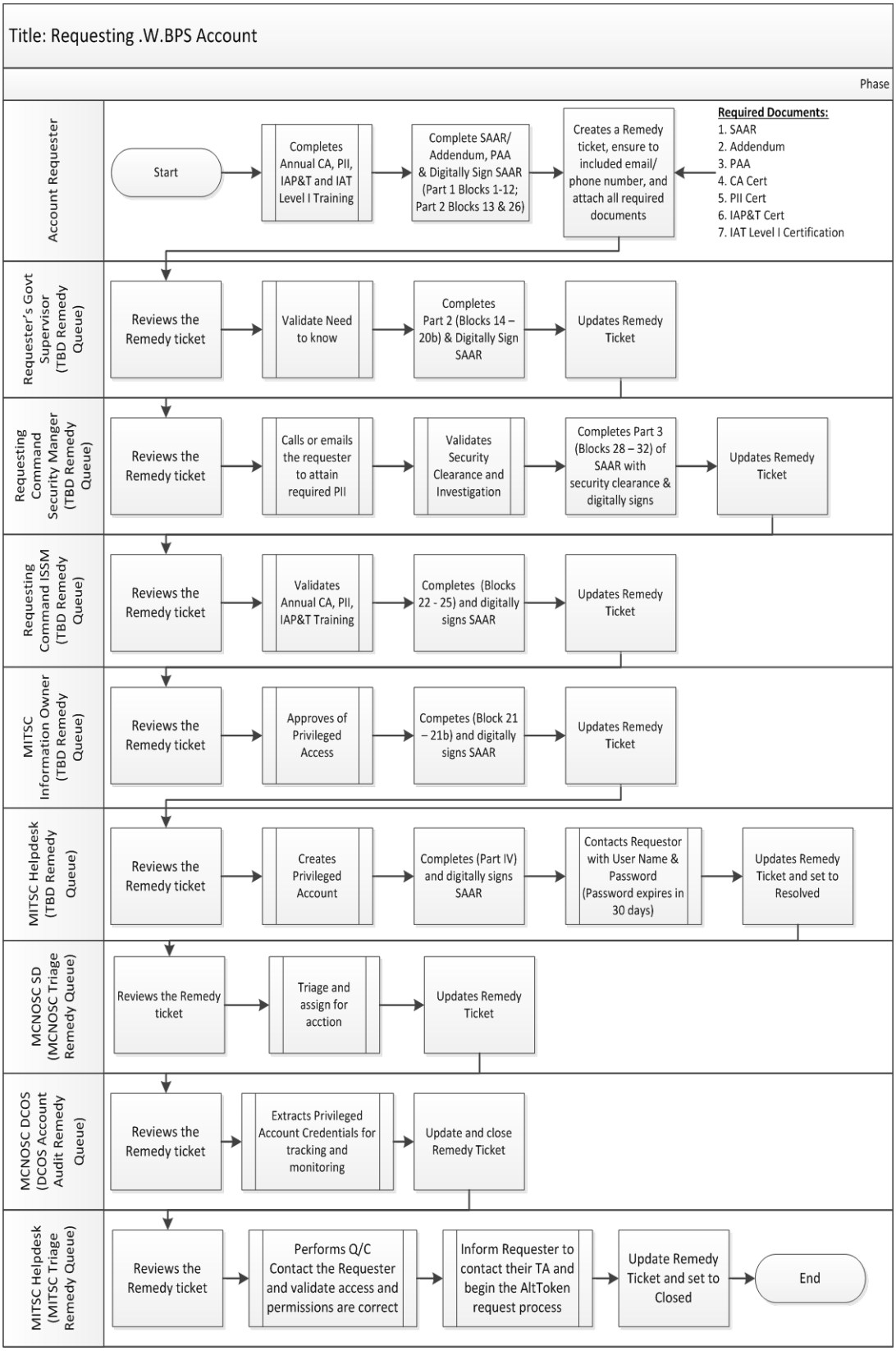
APPENDIX H — REQUESTING .S.MIT ACCOUNT WORKFLOW



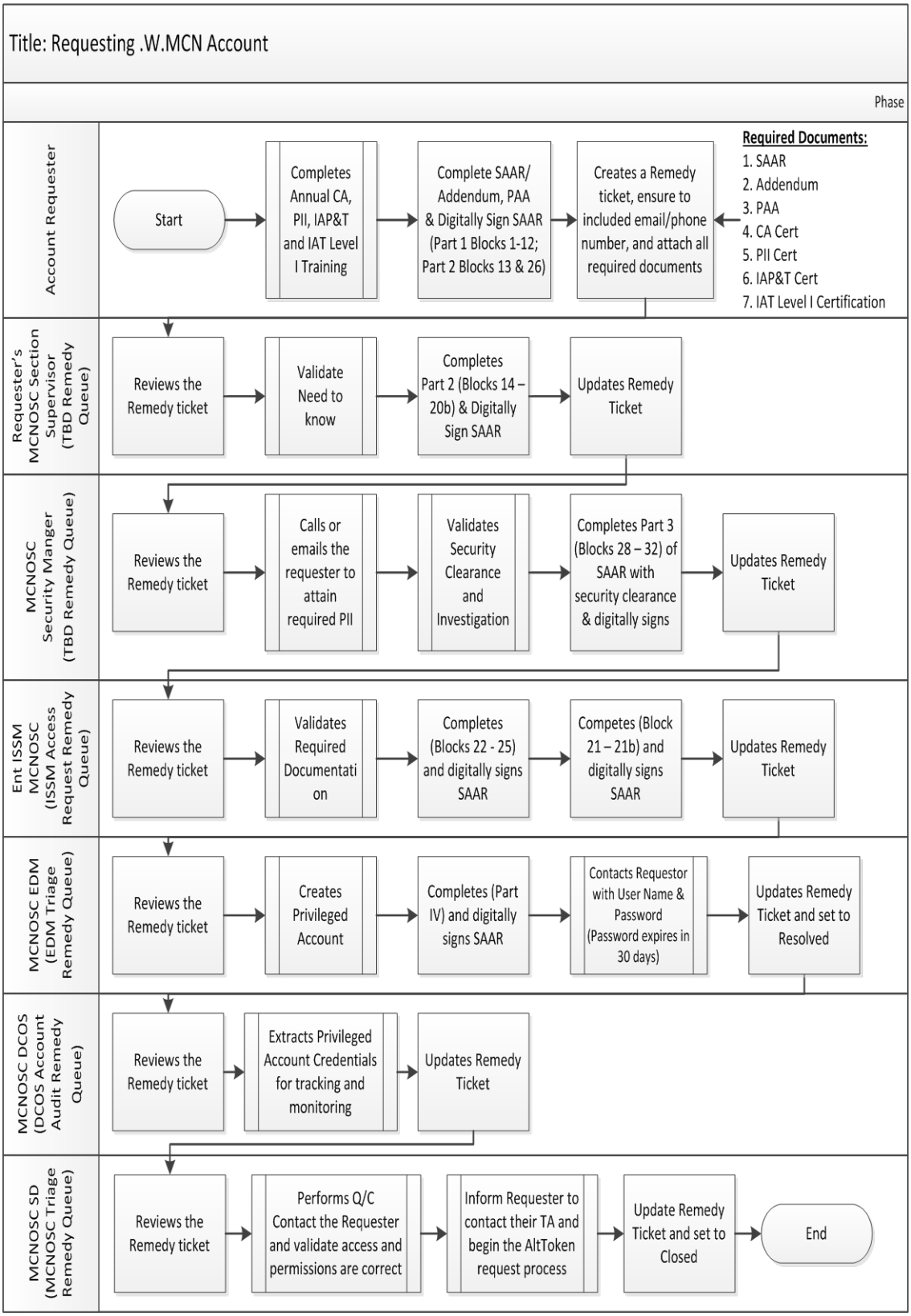
APPENDIX I — REQUESTING .S.TSC ACCOUNT WORKFLOW



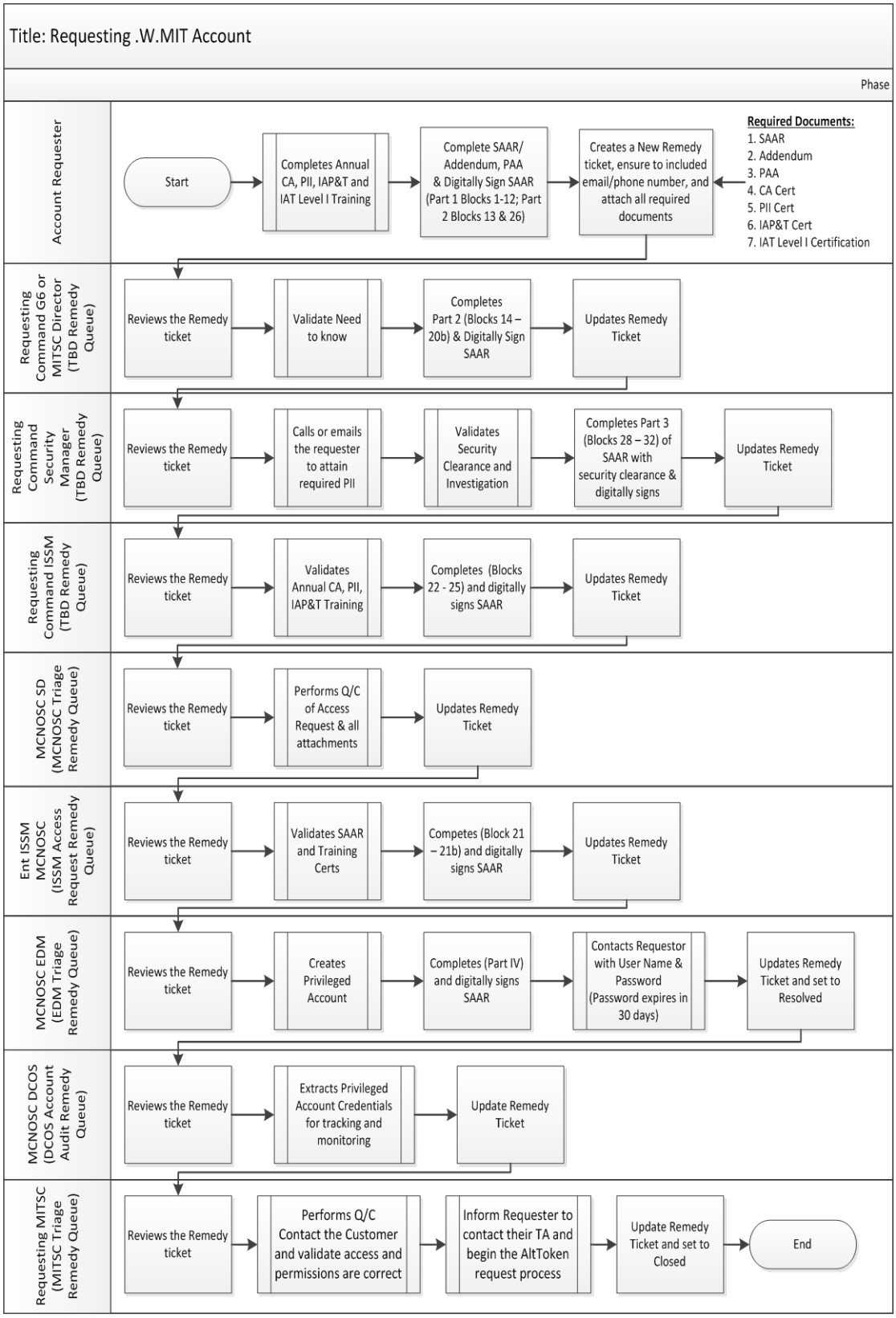
APPENDIX J — REQUESTING .W.BPS ACCOUNT WORKFLOW



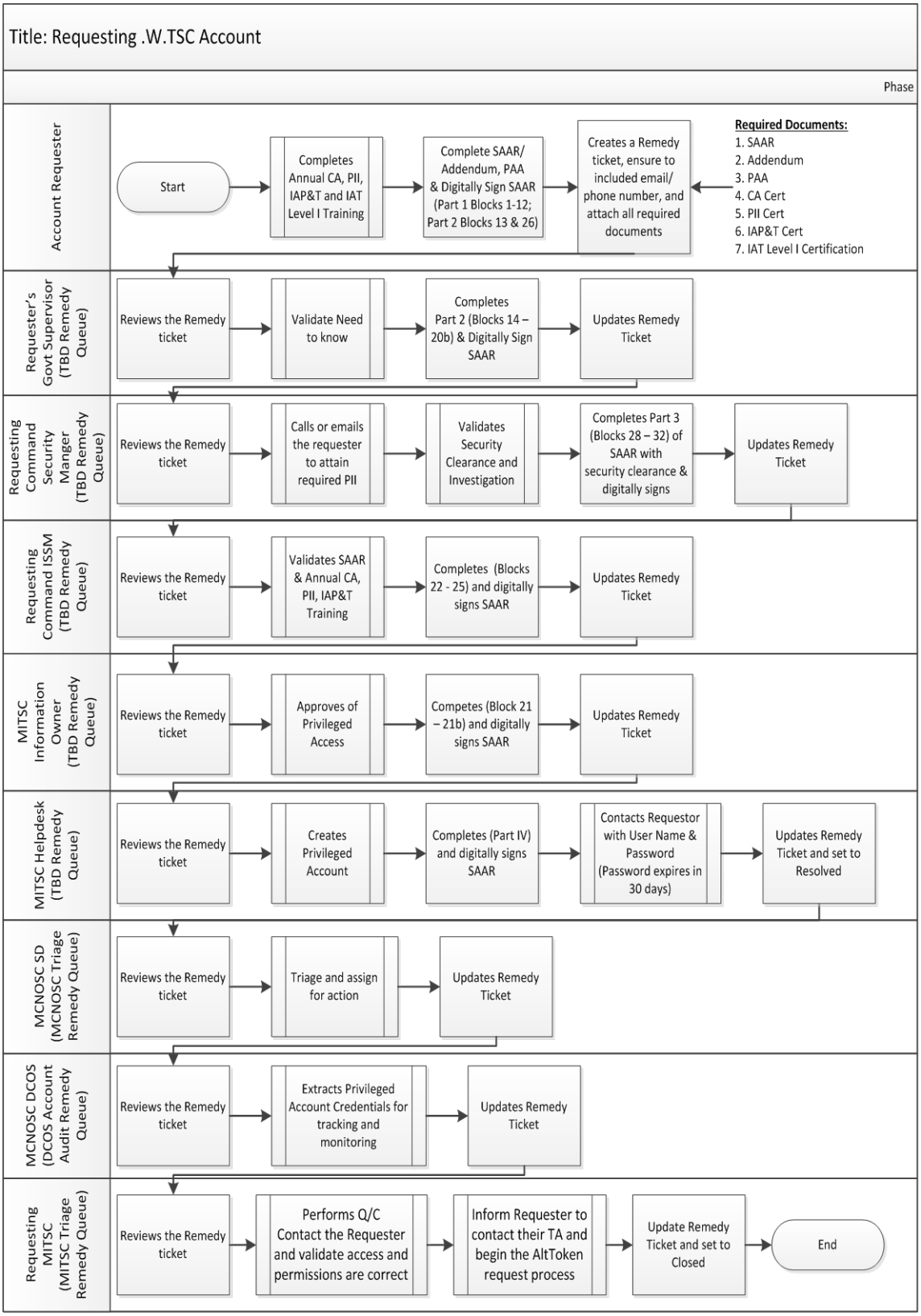
APPENDIX K — REQUESTING .W.MCN ACCOUNT WORKFLOW



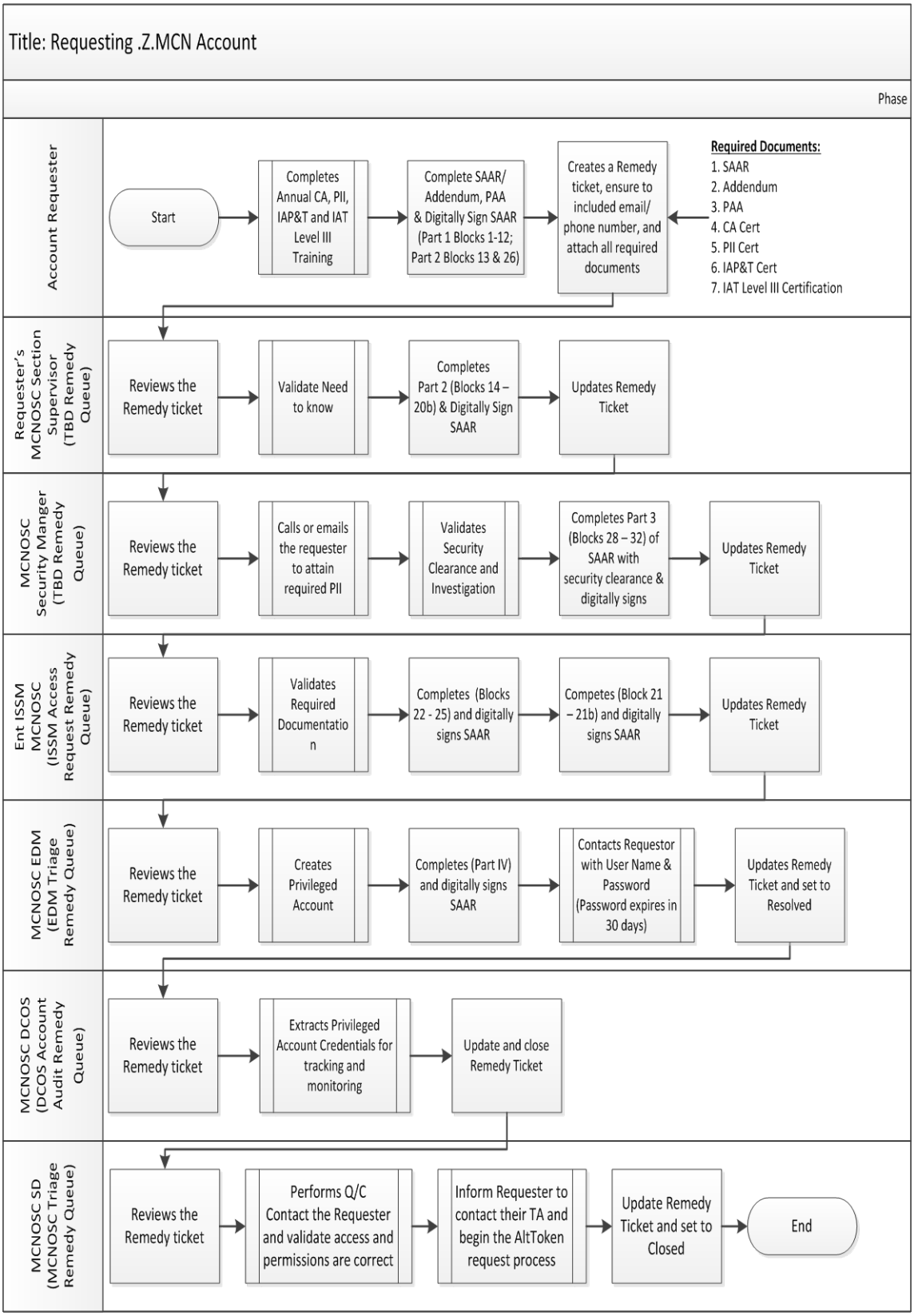
APPENDIX L — REQUESTING .W.MIT ACCOUNT WORKFLOW



APPENDIX M — REQUESTING .W.TSC ACCOUNT WORKFLOW



APPENDIX N — REQUESTING .Z.MCN ACCOUNT WORKFLOW



APPENDIX O — REFERENCES

In meeting and achieving this process guidance, the following directives and documentation should be referenced to ensure compliance and support for the implementation of the Identity and Access Management (IAM) process.

- ITIL v3 Service Operations
- Identity and Access Management (IdAM) Strategy Draft Version 1.0
- Department of Defense Information Enterprise Architecture Identity and Access Management Reference Architecture Draft Version 1.0
- SECNAV_5239
- DODI 8500.2
- SECNAVINST 5239.3B
- Enterprise IT Service Management Incident Management Process Guide
- MARADMIN 690/13
- MCEN Transition Strategy, July 2013
- Incident Management Process Guide
- MARADMIN 098/10
- CNATRAINST 5230.4A
- DoD Approved 8570 Baseline Certifications <http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html>
- DEPSECDEF Memorandum, Joint Information Environment Implementation, May 06, 2013
- DoD Chief Information Officer (CIO) Memorandum, Department of Defense Requirements for Accepting Non-Federally Issued Identity Credentials. June 24, 2013
- DoD CIO Memorandum, DoD Identity Protection and Management Senior Coordinating Group, DoD IdM Strategic Plan, August 20, 2009
- DoD CIO Memorandum, Requirements for Public Key Infrastructure Certificates for Non-Person Entities on the Non-classified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet). May 10, 2013
- DoD Identity Assurance (IdA) CONOPS v1.0. September 25, 2012
- DoD Identity Management Strategic Plan. April, 2009
- DoD Directive (DoDD) 1000.25, DoD Personnel Identity Protection (PIP) Program. April 23, 2007
- DoDD 5200.43, Management of the Defense Security Enterprise. October 1, 2012
- DoD Enterprise-wide Access to Network and Collaboration Services Version 1.0. December, 2009
- DoD Enterprise User Data Management Plan for Persons and Personas v1.0. August 9, 2010
- DoD ITESR Version 1.0, September 6, 2011
- DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information. October 9, 2008
- DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB).DoDI 8320.02, Sharing of Data, Information and Information Technology in the DoD, August 5, 2013
- DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling. May 24, 2011

- DoDI 8520.03, Identity Authentication for Information Systems. May 13, 2011
- DoD Manual 5200.01, Volumes 1-4, DoD Information Security Program, February 24, 2012
- DoD Privilege Management Roadmap, January 6, 2010
- DoD Security Lexicon, Office of the Undersecretary of Defense, Intelligence, June 13, 2013
- Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. October 7, 2011
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0. December 2, 2011
- Federal Information Processing Standard (FIPS) 201-2, August 2013
- Global Information Grid 2.0 Initial Capabilities Document, June, 2009
- Identity, Credential, and Access Management (ICAM) Lexicon, Version 1.0, Prepared by the National Security Systems Identity, Credentialing and Access Management (ICAM) Focus Group, May 30, 2013
- JIE Operations CONOPS. January 25, 2013
- National Strategy for Information Sharing and Safeguarding. December, 2012
- National Strategy for Trusted Identities in Cyberspace. April, 2011
- United States Code. The Privacy Act of 1974.December 31, 1974
- Cisco Secure Access Control Server Account Escalation Procedure v1.0.3, February 8, 2013
- MCEN Network Password Procedure v 1.0.2, April 5, 2013
- MCEN Network Account Management Procedure v1.0.2, April 5, 2013