

USAREC Pamphlet 25-1-1

**Information Management: Business Roles,
Processes and Procedures**

**USAREC
Information
Technology
Implementation
Instructions**

**Headquarters
United States Army Recruiting Command
Fort Knox, Kentucky
5 June 2017**

UNCLASSIFIED

SUMMARY of CHANGE

USAREC Pam 25-1-1 Information Technology Implementation Instructions:
This administrative revision, dated 31 Dec 2019, supersedes the initial published version of the UP 25-1-1.—

Cybersecurity

- o Figure 2-8 deleted
- o Figures 8-13 Re-numbered

ITBO:

- o Governance Division changed to Information Technology Business Office throughout publication.
- o Figures 3-1 thru 3-8: Updated.
- o Figures 3-9 and 3-10: New (CP-34 Registration and Outreach).

OPERATIONS:

- o Figure 4-2: Updated (RFS for Telecomms).

ISD:

- o Figure 5-7: New (Offline Device Enrollment-CHESS Software Request Process).
- o Figure 5-8: New (Offline Device Enrollment-MaaS360 Process).
- o Figure 5-9: New (VTC Request Process).
- o Figure 5-10: New (Software Center Quick Start Guide for Recruiters).
- o Figure 5-11: Removed (Thumb drive Imaging Process) o Figure 5-11 (Prev Fig. 5-12): HQ IT Support Request Process.

P3MD:

- o Figure 6-1: New (P3MD Structure).
- o Figure 6-1 became 6-2
- o Figure 6-2 became 6-3
- o Figure 6-3 became 6-4
- o Figure 6-4 became 6-5

Headquarters
United States
1307 3rd Avenue
Fort Knox, Kentucky 40121-2725
12 December 2019

***USAREC Pamphlet 25-1-1**

Effective Date: 12 December 2019

Information Management: Business Roles, Processes, and Procedures

USAREC Information Technology Implementation Instructions

For the Commander:

CARTER L. PRICE
Colonel, GS
Chief of Staff

Applicability. This pamphlet is applicable to all elements of the United States Army Recruiting Command.

Publications and Blank Forms) directly to HQ USAREC, ATTN: RCIO, 1307 3rd Avenue, Fort Knox, KY 40121-2725; or by e-mail to: usarmy.knox.usarec.list.hq-g6-pubs@mail.mil

Official:

Ronnie L. Creech
Assistant Chief of Staff, CIO/G6

Proponent and exception authority. The proponent of this pamphlet is the Chief information officer, G-6. The proponent has the authority to approve exceptions to this pamphlet that are consistent with controlling law and regulation. Proponents may delegate the approval authority, in writing, to a Division Chief within the proponent agency in the grade of Lieutenant Colonel or the civilian equivalency.

Relation to USAREC Reg. 10-1. This pamphlet establishes policies and procedures regarding Information Management: Business Roles, Processes, and procedures, according to USAREC Reg. 10-1 para 3-16b.

History. This is an expedite revision dated 12 December 2019

Summary. This pamphlet explains the business roles, procedures, and implementation instructions for the process which the G-6, United States Army Recruiting Command is responsible.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to

Supplementation

Supplementation of this pamphlet is prohibited.

Distribution. This pamphlet is only available in electronic media.

This pamphlet version 2, supersedes USAREC Pam 25-1-1 V1, dated 5 June 2017

UNCLASSIFIED

Contents (Listed by paragraph and page number)

Chapter 1.

Purpose • 1-1, *page 1*

References • 1-2, *page 1*

Explanation of abbreviations and terms • 1-3, *page 1*

Organization and Responsibilities • 1-4, *page 1*

Records Management Requirements • 1-5, *page 1*

Pamphlet structure • 1-6, *page 1*

Chapter 2. G-6 Cybersecurity Division Roles and Business Processes.

The Cybersecurity Division (CSD) • 2-1, *page 2*

Cyber Policy Branch Roles • 2-2, *page 2*

Cybersecurity Branch roles • 2-3, *page 2*

Cyber Division business processes are listed below • 2-4, *page 2*

Chapter 3. G-6 Information Technology Business Office.

Information Technology Business Office (ITBO) • 3-1, *page 15*

IT Resources Branch roles • 3-2, *page 15*

Information Technology Business Office roles • 3-3, *page 15*

Information Technology Business Office Division Business Processes • 3-4, *page 15*

Chapter 4. G-6 Operations Division Roles and Business Processes.

The Operations Division • 4-1, *page 26*

Network Operations Branch roles • 4-2, *page 26*

IT Plans Branch roles • 4-3, *page 26*

Operations Division Business • 4-4, *page 26*

Chapter 5. G-6 Integrated Solutions Division.

Integrated Solutions Division • 5-1, *page 29*

IPAD DRMO process • 5-2, *page 29*

Chapter 6. G-6 Product, Program and Project Management Division (P3MD) Roles and Functions.

Product, Program and Project Management Division (P3MD) • 6-1, *page 41*

P3MD is comprised of three disciplines • 6-2, *page 41*

List of responsibilities and functions • 6-3, *page 42*

Chapter 7. S-6 Brigade/Battalion Level Roles and Responsibilities.

IT Specialists • 7-1, *page 49*

S-6 • 7-2, *page 49*

Chapter 8. G-6 In/Out Processing Procedures.

- Purpose • 8-1, *page 50*
- Army Acculturation Program • 8-2, *page 50*
- Summary, Scope and Assumptions • 8-3, *page 50*
- In-Processing Responsibilities • 8-4, *page 50*
- Arrival Requirements • 8-5, *page 50*
- Out-Processing Responsibilities • 8-6, *page 51*
- Maintenance • 8-7, *page 52*

Appendixes

- A. Procedures for Removal of SSD Card from Dell Venue Tablets and Tablet Turn in, *page 64*
- B. Guide to verify if Apps are approved for download and Requesting Mobile Apps through USAREC Cybersecurity, *page 68*

Glossary

Figures List (USAREC Processes)

Figure 2-1. USAREC G-6 In/Out Processing Process.....	3
Figure 2-2. Incident Response Process (Theft, loss or compromise of IT Equipment or PII data)	4
Figure 2-3. Comprehensive Management Process.....	5
Figure 2-4. System Authorization Access Request (SAAR) Process-Approved).....	6
Figure 2-5. Cyber Training Request Process	7
Figure 2-6. Cyber Group Mail Boxes Process.....	8
Figure 2-7. Mobile Application Request Process	9
Figure 2-8. REQUEST System Authorization Access Request (SAAR) Process	10
Figure 2-9. Investigation Request Process.....	11
Figure 2-10. Mobile Device Incident Response Process (Theft, Loss or Compromise of Mobility Equipment)	12
Figure 2-11. Mobile Device Compromise APP Leadership Notification Process.....	13
Figure 2-12. Data Retention Process (Investigations)	14
Figure 3-1. ITBO Roles and Responsibilities	16
Figure 3-2. ITBO Business Process.....	17
Figure 3-3. Asset Replacement Process.....	18
Figure 3-4. ITEPS Service Request Process	19
Figure 3-5. New, Revision, or Rescind Publication Process.....	20
Figure 3-6. Business Card Request Process.....	21
Figure 3-7. Freedom of Information Act Process	22
Figure 3-8. CP-34 Registration Process.....	23
Figure 3-9. CP-34 Outreach Process.....	24
Figure 3-10. CP-34 Certification Program Process	25
Figure 4-1. Internal Task Initiation and Tracking Process.....	27
Figure 4-2. USAREC Telecom/RFS Process Flow (Includes new and Replacement Telephones	28
Figure 5-1. Mobility Ticket Process	30
Figure 5-2. MobileIron Process	31
Figure 5-3. LiveScan Device Warranty Replacement Process	32
Figure 5-4. Mobile Support Request (USER) Process.....	33
Figure 5-5. Command Mobility Device Disposition Process	34
Figure 5-6. LiveScan Device Warranty Replacement Process	35
Figure 5-7. Offline Device Enrollment Chess Software Request Process	36
Figure 5-8. Offline Device Enrollment MaaS360 Process	37
Figure 5-9. Video Teleconference Request Process	38
Figure 5-10. Software Center Quick Start Guide for Recruiters.....	39
Figure 5-11. HQ IT Support Request Process	40

Figure 6-1. P3MD Structure	41
Figure 6-2. Products, Programs and Project Management Division (P3MD)-Process Overview.....	44
Figure 6-3. Input of Change into HRC Business Process Request (BQP) Process.....	45
Figure 6-4. End User Testing (EUT) for Major HRC Software Changes Page 1	46
Figure 6-5. End User Testing (EUT) for Major HRC Software Changes Page 2	47
Figure 6-6. Laptop Lifecycle Replacement (LCR) Today	48
Figure 8-1. G-6 In-Processing (Military and DA Civilian)	53
Figure 8-2. G-6 In-Processing (Contract Personnel)	54
Figure 8-3. G-6 Out-Processing (Military and DA Civilian).....	55
Figure 8-4. G-6 Out-Processing (Contract Personnel).....	56
Figure 8-5 . G-6 In-Processing Checklist UF 25-1-1.1	58
Figure 8-6. (Cont.) G-6 User In-Processing Checklist UF 25-1-1.1	59
Figure 8-7. G-6 In-Processing Checklist UF 25-1-1.2.....	59
Figure 8-8. G-6 Directorate Out-Processing Checklist UF 25-1-1.3	60
Figure 8-9. G-6 User Out-Processing Checklist (Military/DA Civilian) UF 25-1-1.4	61
Figure 8-10. G-6 User Out-Processing Checklist (Contract Personnel) UF 25-1-1.5.....	62

Chapter 1.

1-1. Purpose

This pamphlet provides operational procedures and practical guidance to USAREC organizations and activities for the use of Information Management (IM) and Information Technology (IT) products, services and support. This includes interactions with IT service providers supporting the command, use of the DOD Information Network (DODIN), Army Information Systems (AIS), the Recruiting Services Network (RSN), and support of end-users.

1-2. References

See appendix A.

1-3. Explanation of abbreviations and terms

See glossary.

1-4. Organization and Responsibilities

a. The CIO and ACoS, G-6 is the principal staff officer for all information technology and information management matters necessary for the execution of the USAREC mission. The G-6 develops and integrates command-wide information technology and information management plans, policies and procedures that enable the accomplishment of the USAREC mission sets through the effective application of command, control, communications, and computer (C4) capabilities. The G-6 is the staff proponent for all matters relating to IM and IT assets, applications, and services, and ensures that all IT efforts are vetted, approved, and prioritized. The G-6 provides a holistic view and oversight of all IT efforts ensuring they support the priorities and initiatives of the Commanding General, while executing duties inherent to and within the G-6.

b. All IT investments including systems change requests, change management, release management, and new IT development and acquisitions will have G-6 oversight, management, and approval prior to execution. In areas of shared responsibility, G-6 will coordinate with the appropriate service providers to track outages, resolutions, and technical reasons for outage. G-6 will provide a description of the technical outages to system users, all staff directors and deputies, and to the Chief of Staff. G-6 will also provide frequent and recurring updates on critical IT events as they develop or upon request. The G-6 prepares Annex H (Signal) to the annual USAREC Operation Order.

1-5. Records Management Requirements

As decreed by AR 25-400-2, the records management (recordkeeping) requirements for all record numbers, associated forms, and reports are included in the Army's Records Retention Schedule-Army (RRS-A). Detailed information for all related record numbers, forms, and reports associated with AR 25-30 are located in RRS-A at <https://www.arims.army.mil>. (See records management requirements in para 2-12.)

1-6. Pamphlet structure

a. The CIO/G-6 Information Management Directorate (IMD) is comprised with five Divisions as listed below, and each Division has its own chapter in this publication:

- (1) Cybersecurity/Information Assurance (Chapter 2)
- (2) Information Technology Business Office (Chapter 3).
- (3) Operations (Chapter 4).
- (4) Integrated Solutions Division (Chapter 5).
- (5) Products, Programs and Project Management (Chapter 6).

b. Chapter 7 Roles and responsibilities of the S-6 staffs for Brigades and Battalions

c. Chapter 8 standardizes policies and procedures for the processing of personnel in and out of the command

Chapter 2.

G-6 Cybersecurity Division Roles and Business Processes.

2-1. The Cybersecurity Division (CSD)

ISD consists of the Cyber Policy Branch and Cybersecurity Branch. Both branches have certain roles as they apply to USAREC, the G-6 directorate, and are listed below.

2-2. Cyber Policy Branch Roles:

- a. Advise the G-6 leadership team.
- b. Acceptable User Policy management.
- c. Development of cyber policy.
- d. Management and oversight of commercial RSN user secondary accounts with elevated privileges.
- e. Attend service provider cyber briefings.
- f. Recommend future direction.
- g. Policy and compliance management.
- h. Compliance with IT regulations and public law.
- i. Accounts management.

2-3. Cybersecurity Branch roles.

- a. Information Security-response to Serious Incident Reports (SIR).
- b. Cyber Awareness Training Management.
- c. Cyber tasking's.
- d. TRADOC Cyber Center of Influence (COI) Training Attendance.
- e. Personally Identifiable Information (PII) in Digital Communications.

2-4. Cyber Division business processes are listed below.

- a. USAREC G-6 In /Out Processing (see figure 2-1).
- b. Incident response process for theft, loss or compromise of IT equipment and/or PII data. (See figure 2-2)
- c. Comprehensive Incident Management Process (see figure 2-3)
- d. System Authorization Access Request Process-Approved (see figure 2-4)
- e. Cyber Training Request Process (see figure 2-5)
- f. DEE NPE Organizational Group Mailboxes Process (Secure) (see figure 2-6)
- g. Mobile Application Request Process (see figure 2-7)
- h. REQUEST System Authorization Access Request (SAAR) Process (see figure 2-8)
- i. Investigation Request Process (see figure 2-9)
- j. Mobile Device Incident Response Process (see figure 2-10)
- k. Mobile Device Compromise Process (Theft, Loss or Compromise of Mobility Equipment) (see figure 2-11)
- l. Data Retention Process (Investigations) (see figure 2-12)

Figure 2-1 In/Out Processing

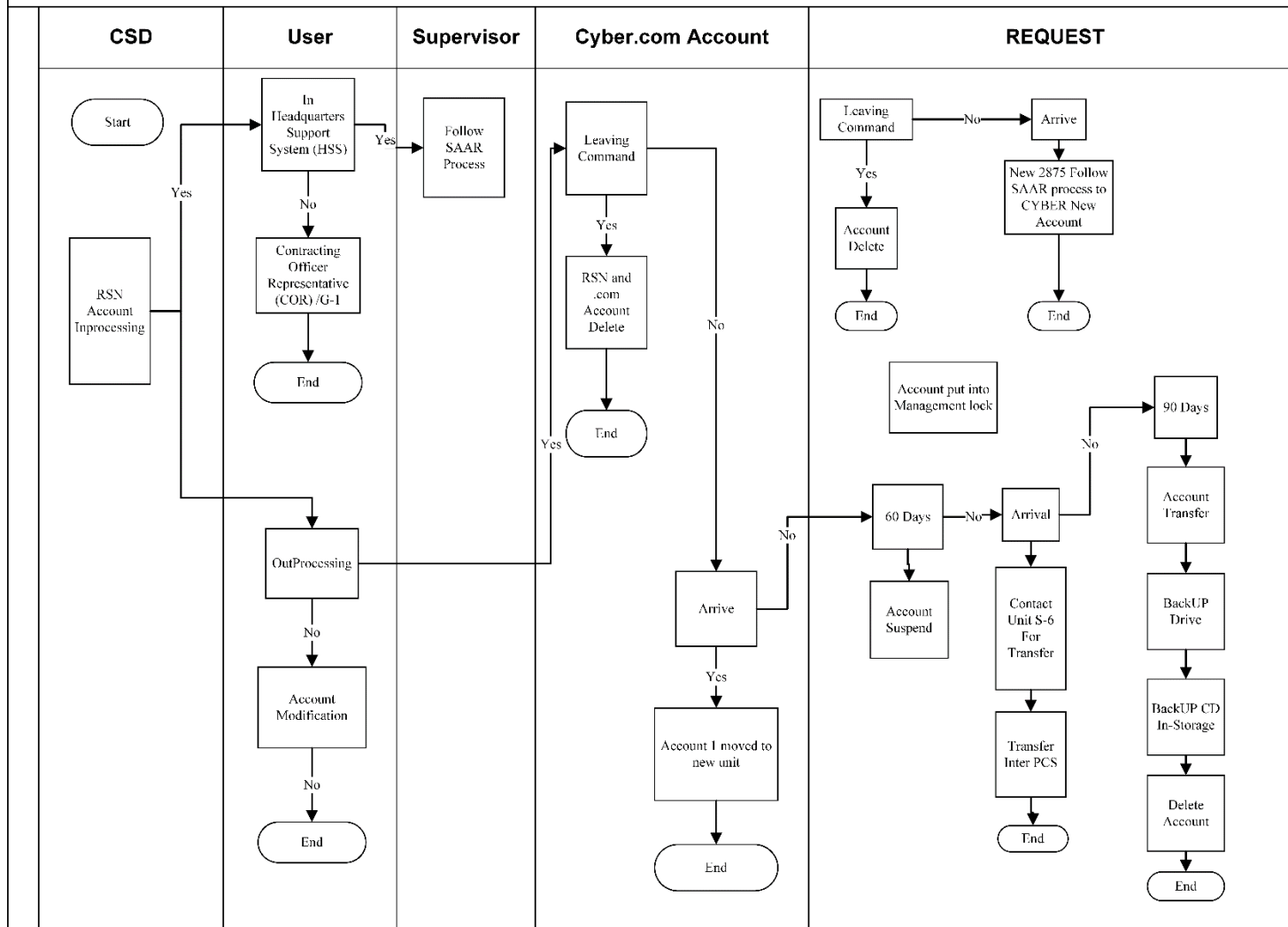


Figure 2-1. USAREC G-6 In/Out Processing Process

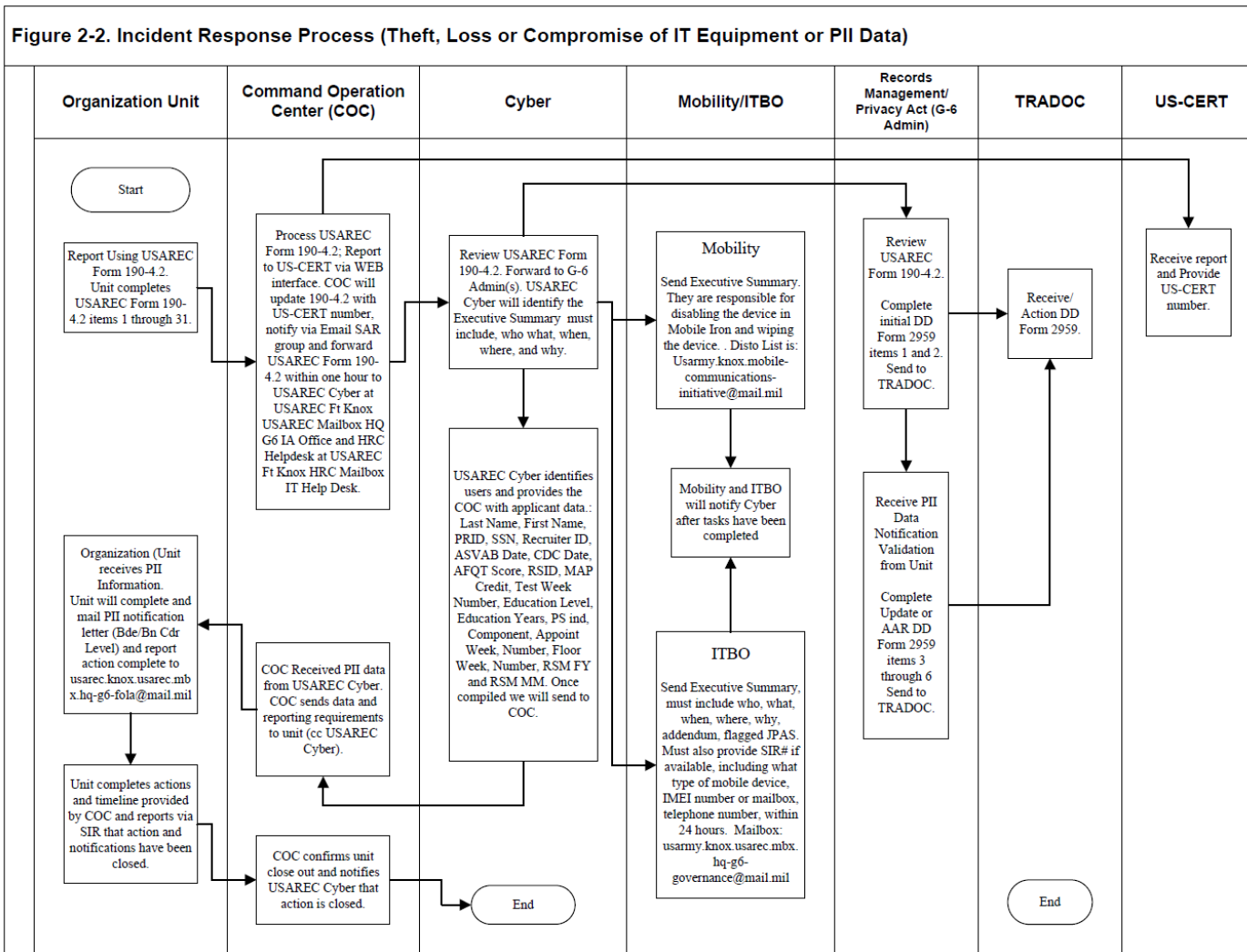


Figure 2-2. Incident Response Process (Theft, loss or compromise of IT Equipment or PII data)

Figure 2-3. Comprehensive Management Process

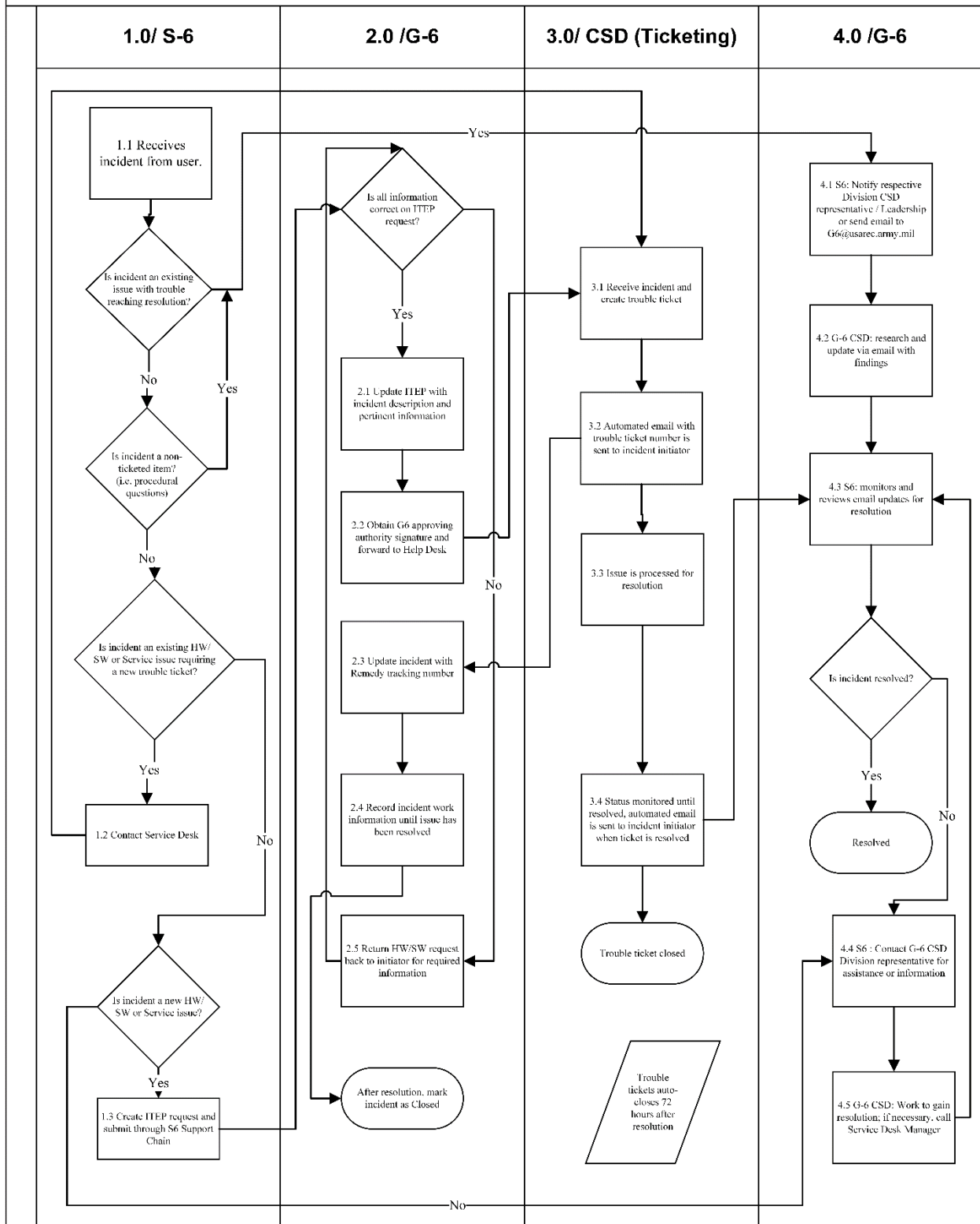


Figure 2-3. Comprehensive Management Process

Figure 2-4. System Authorization Access Request (SAAR) Process

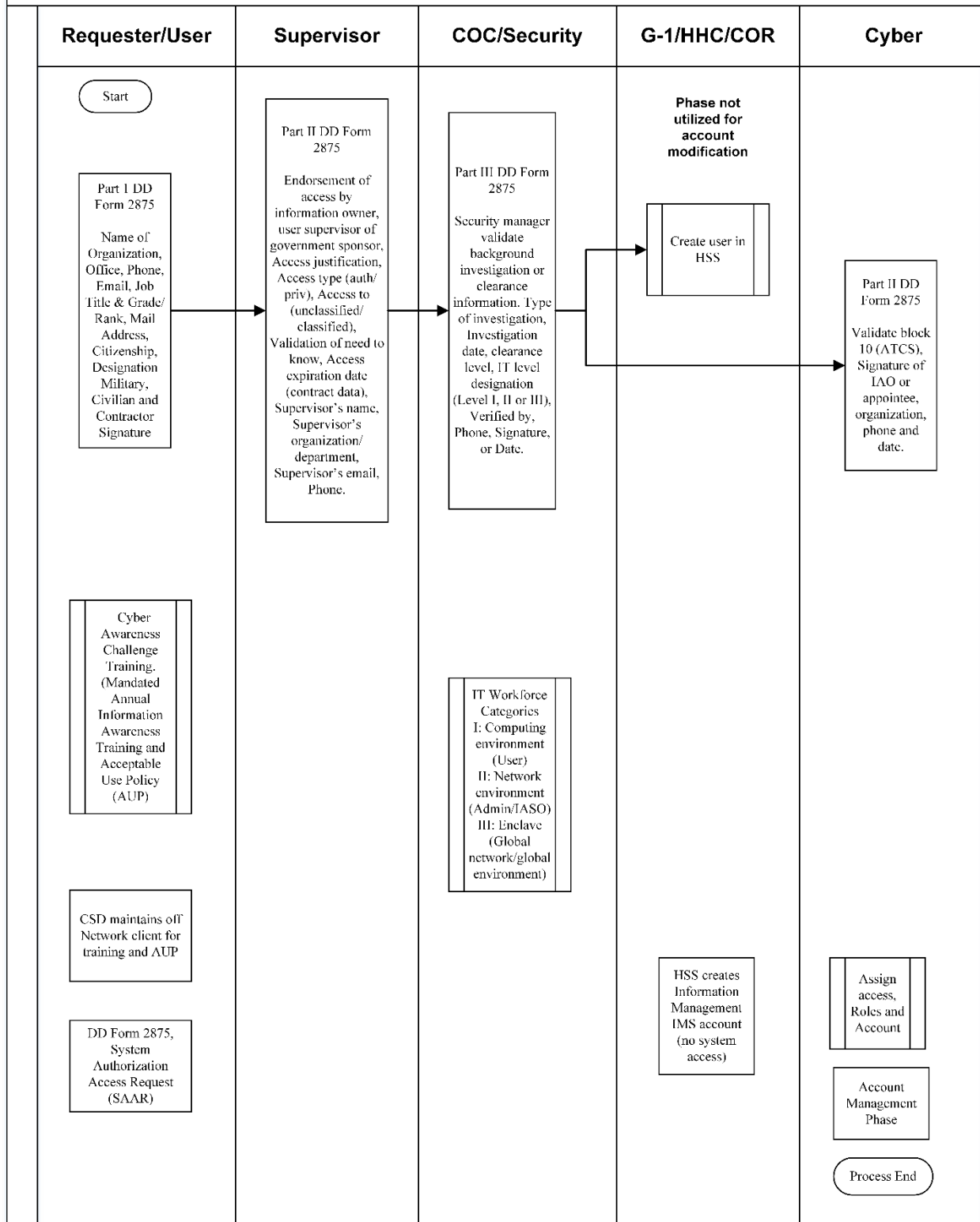


Figure 2-4. System Authorization Access Request (SAAR) Process-Approved)

Figure 2-5. Cyber Training Request Process

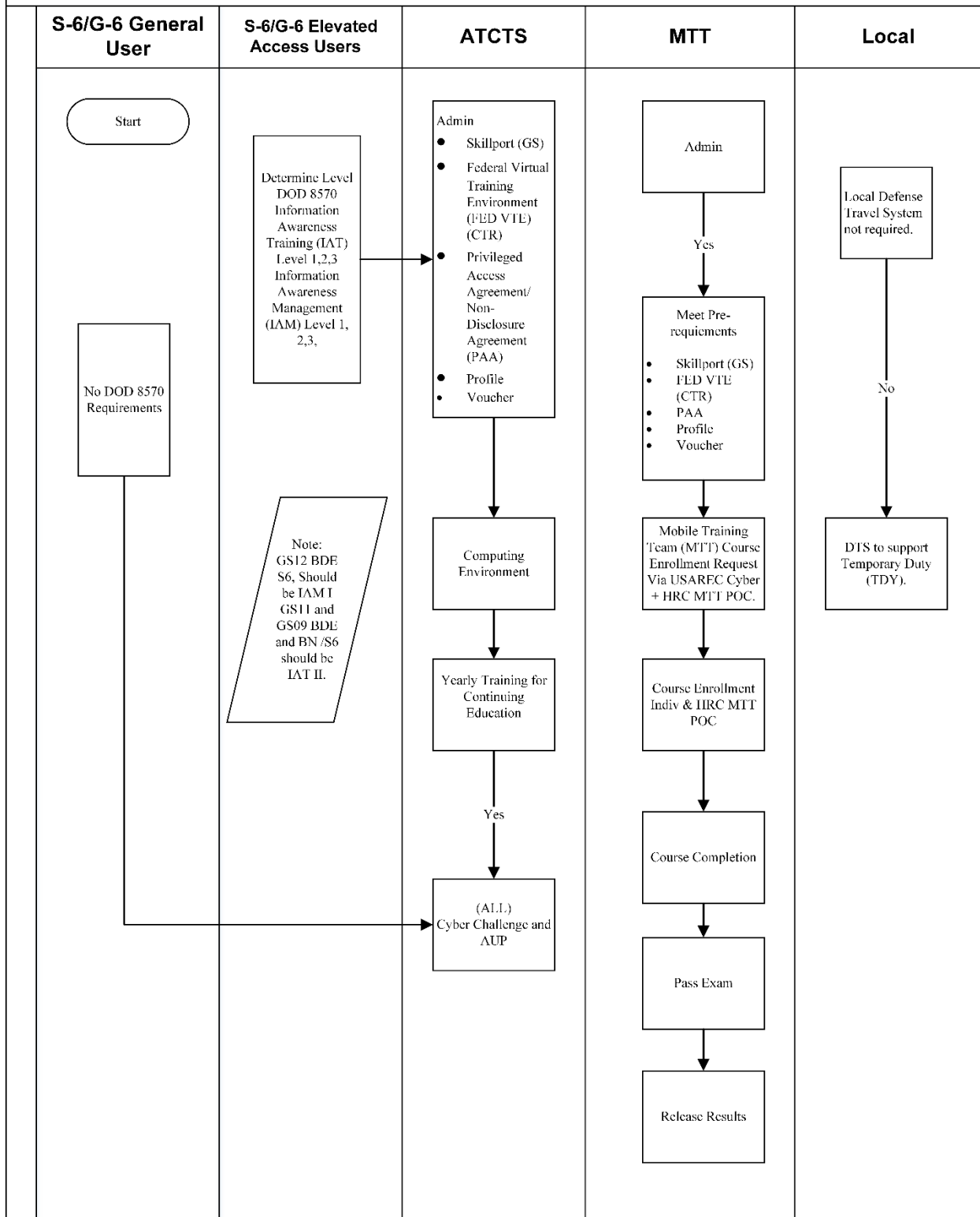


Figure 2-5. Cyber Training Request Process

Figure 2-6 Cyber Group Mail Boxes Process

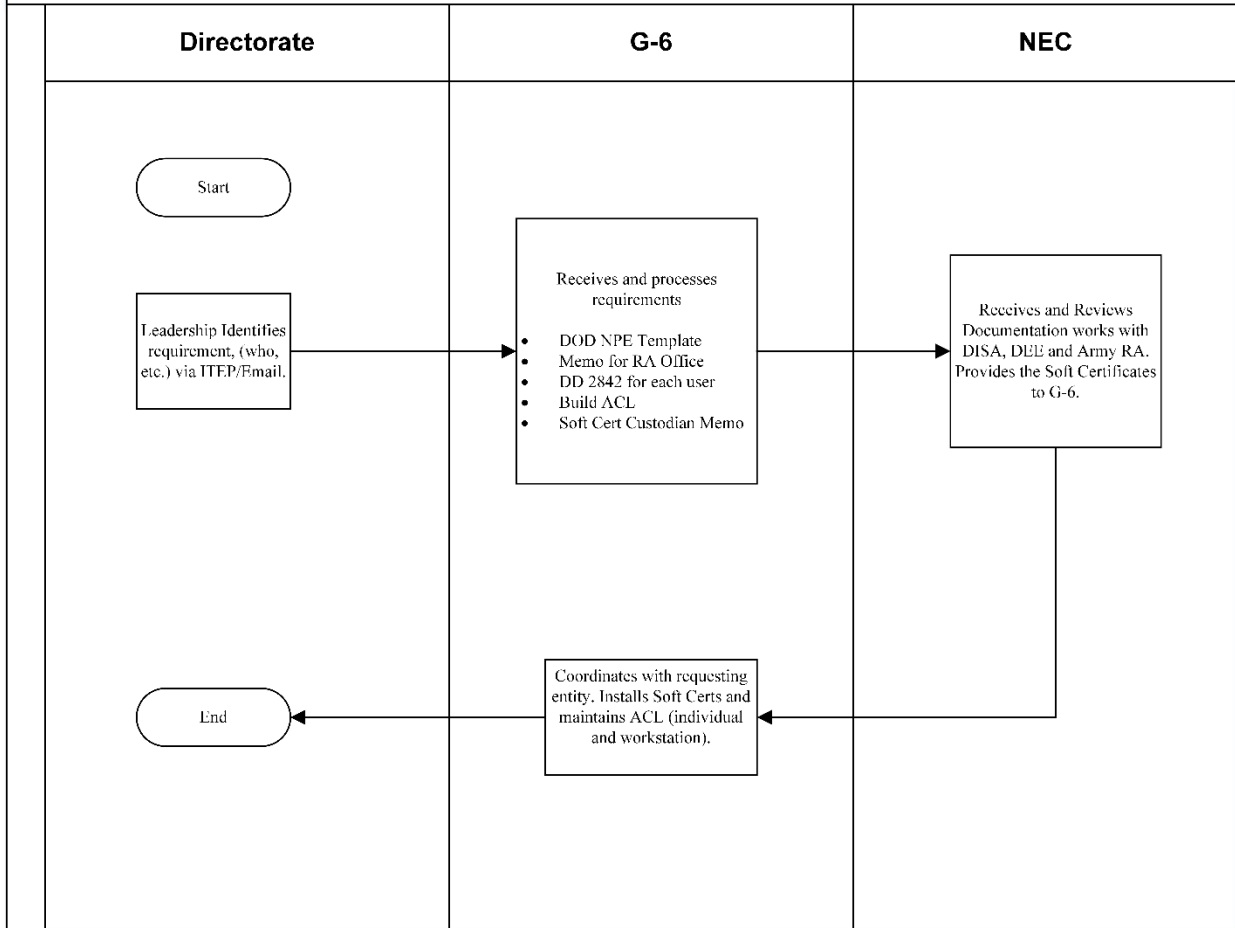


Figure 2-6. Cyber Group Mail Boxes Process

Figure 2-7. Mobile Application Request Process

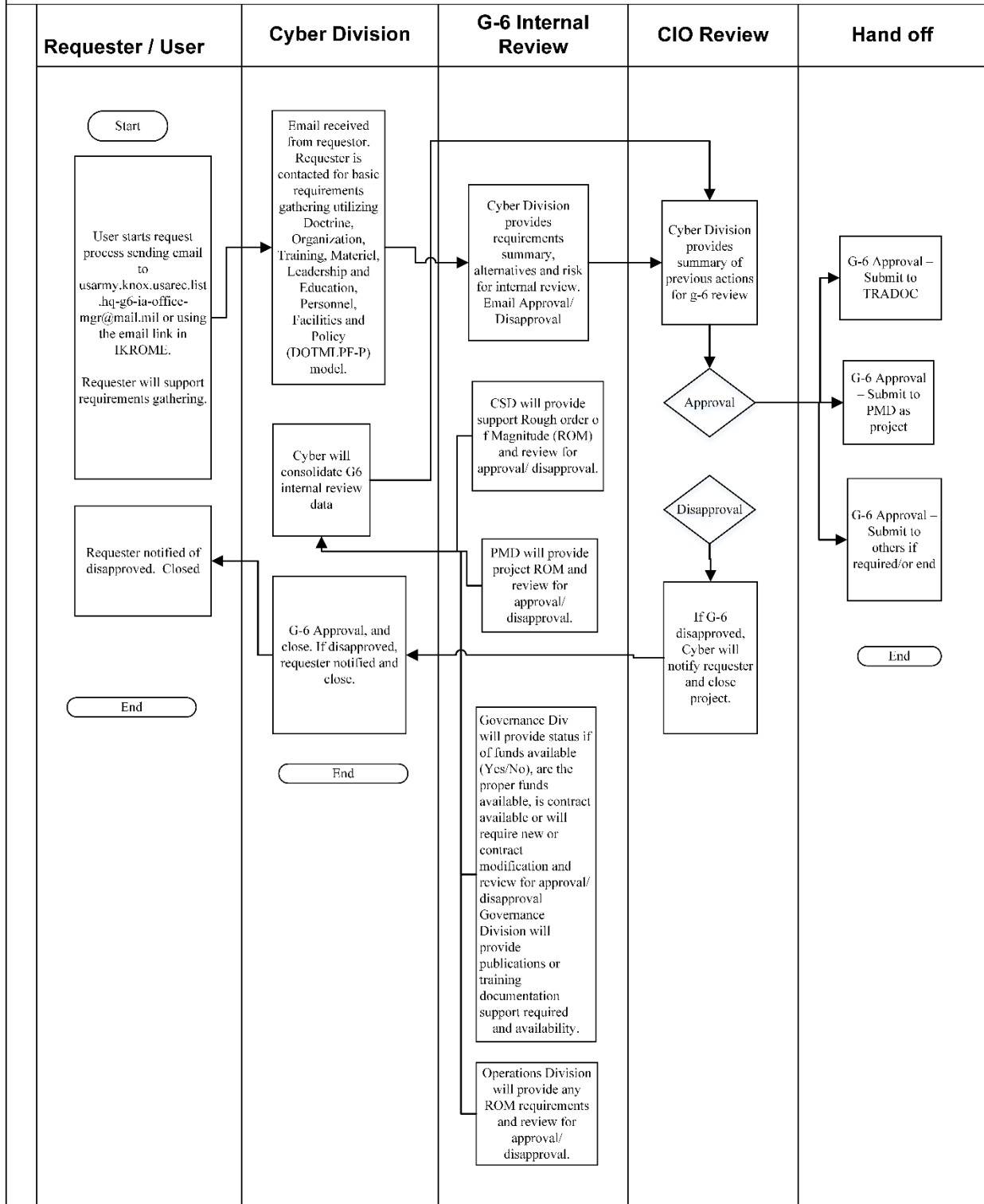


Figure 2-7. Mobile Application Request Process

Figure 2-8. REQUEST System Authorization Access Request (SAAR) Process

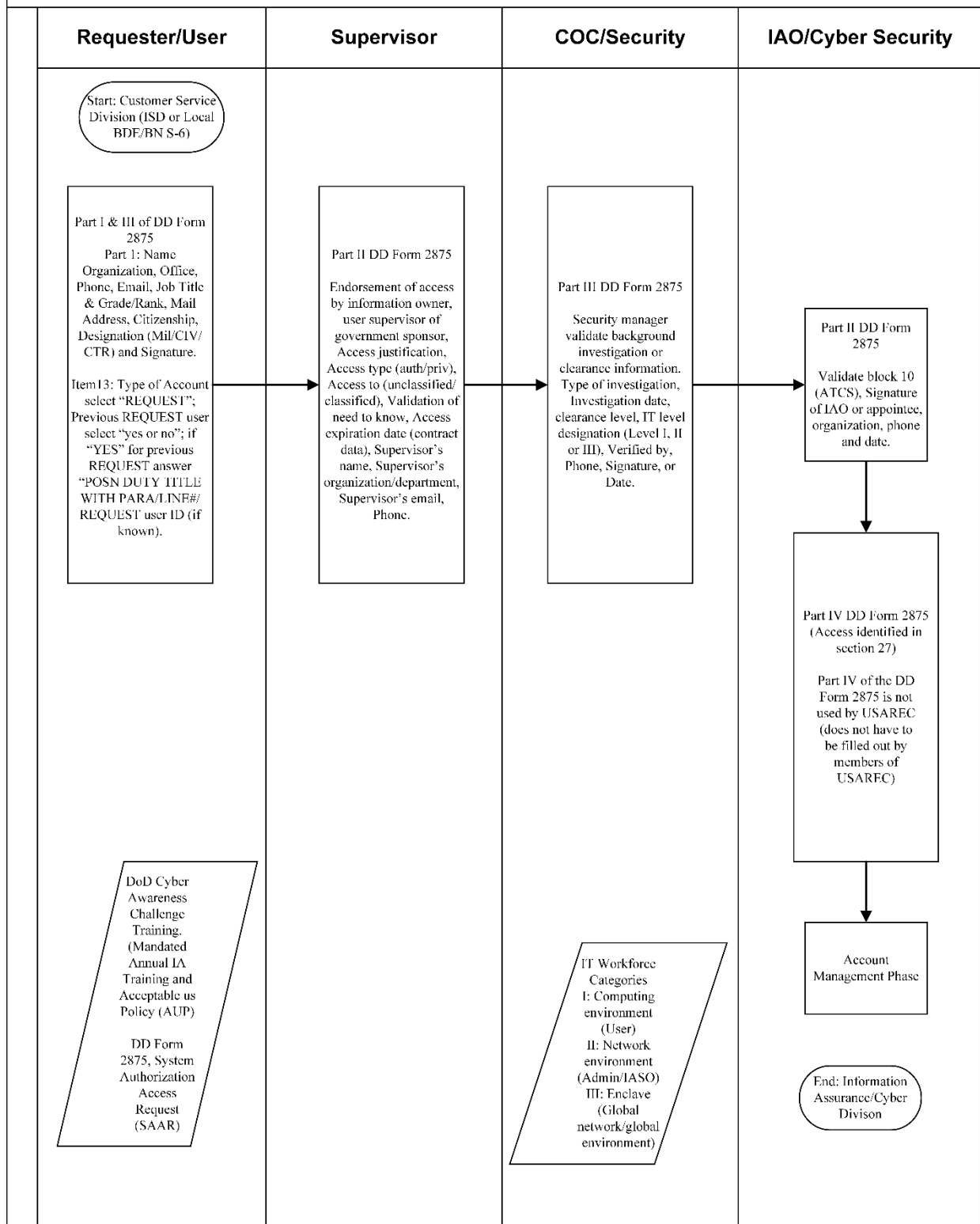


Figure 2-8. REQUEST System Authorization Access Request (SAAR) Process

Figure 2-9. Investigation Request Process

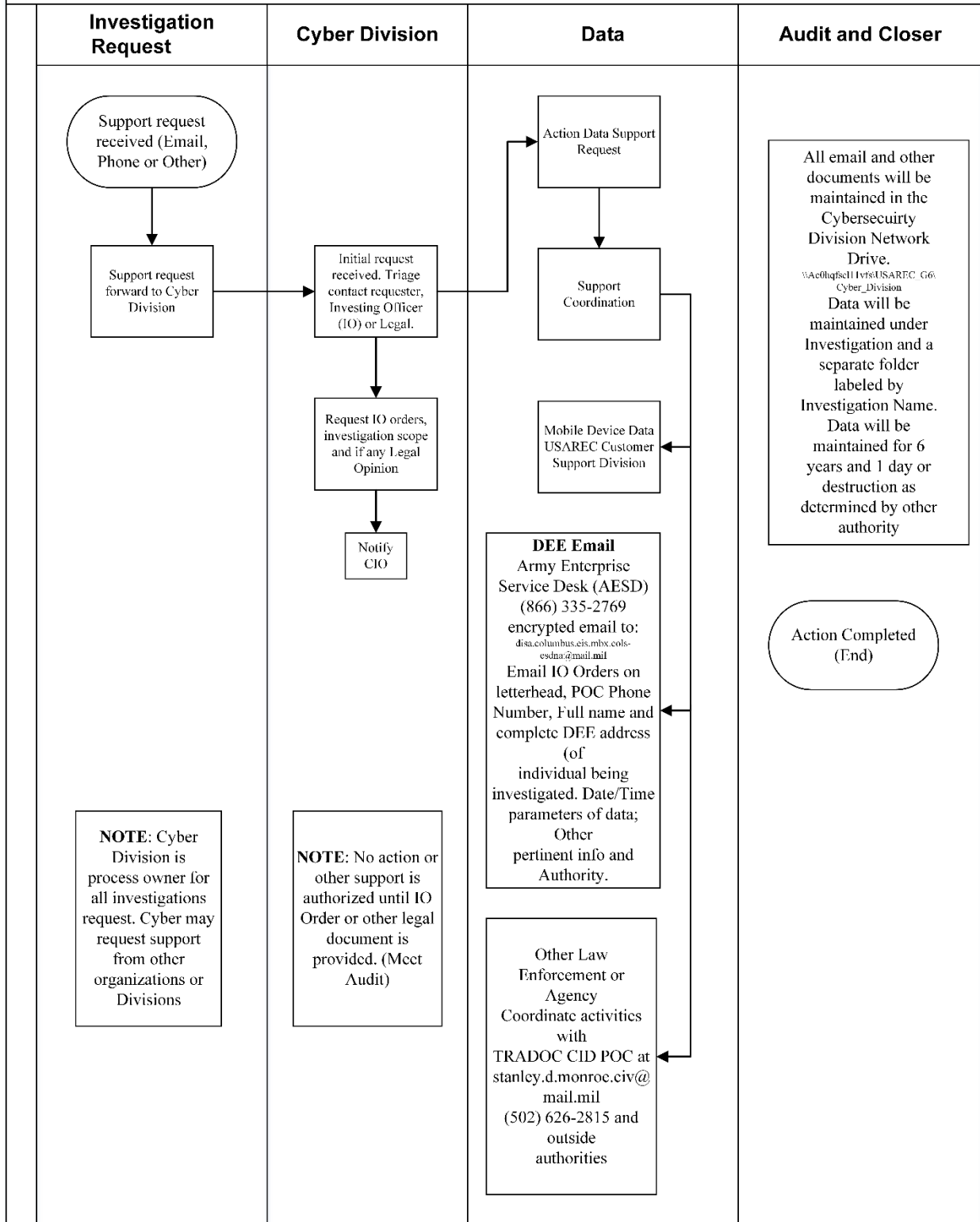


Figure 2-9. Investigation Request Process

Figure 2-10. Mobile Device Incident Response Process (Theft, Loss or Compromise of Mobility Equipment)

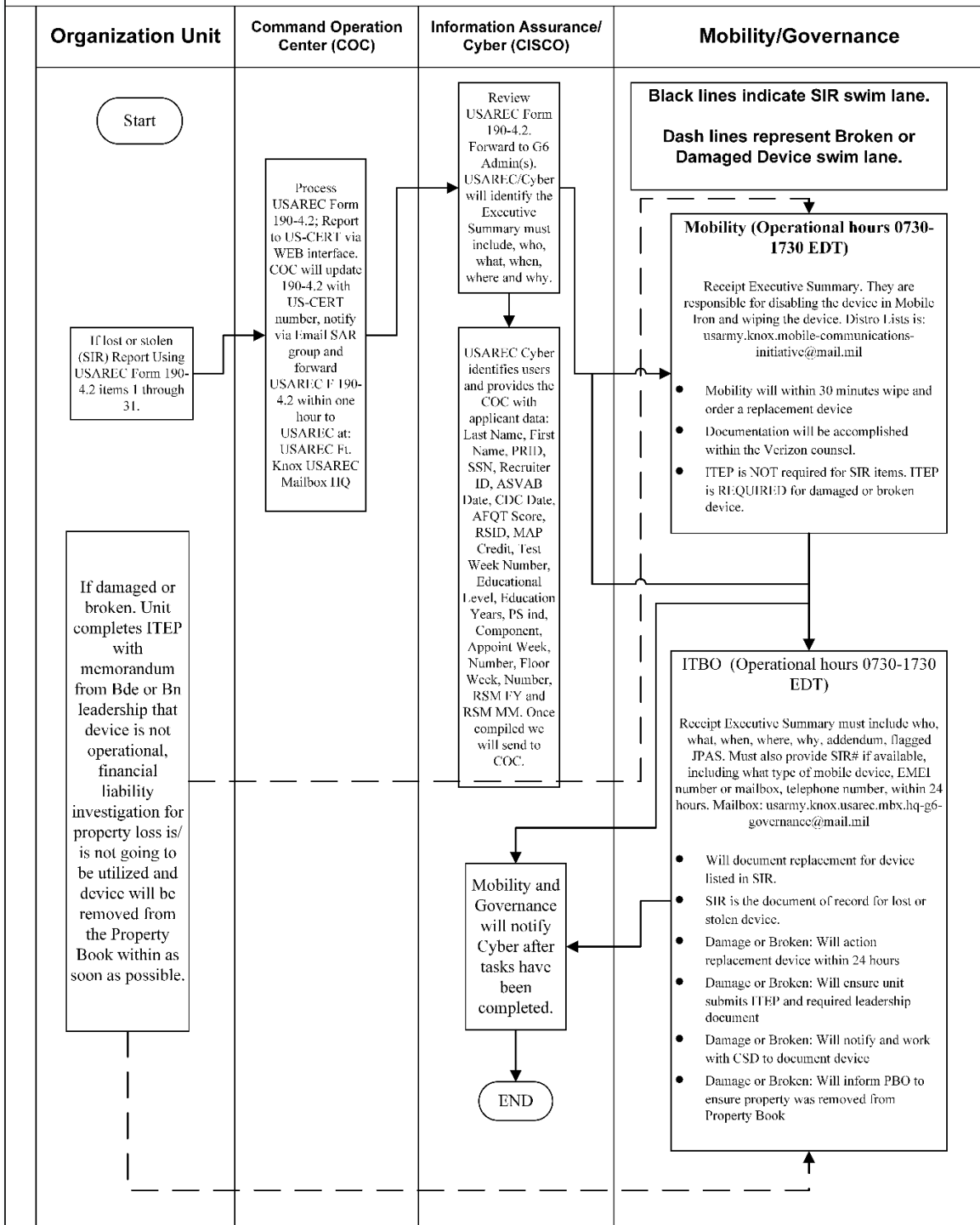


Figure 2-10. Mobile Device Incident Response Process (Theft, Loss or Compromise of Mobility Equipment)

Figure 2-11. Mobile Device Compromise (APP) Leadership Notification Process

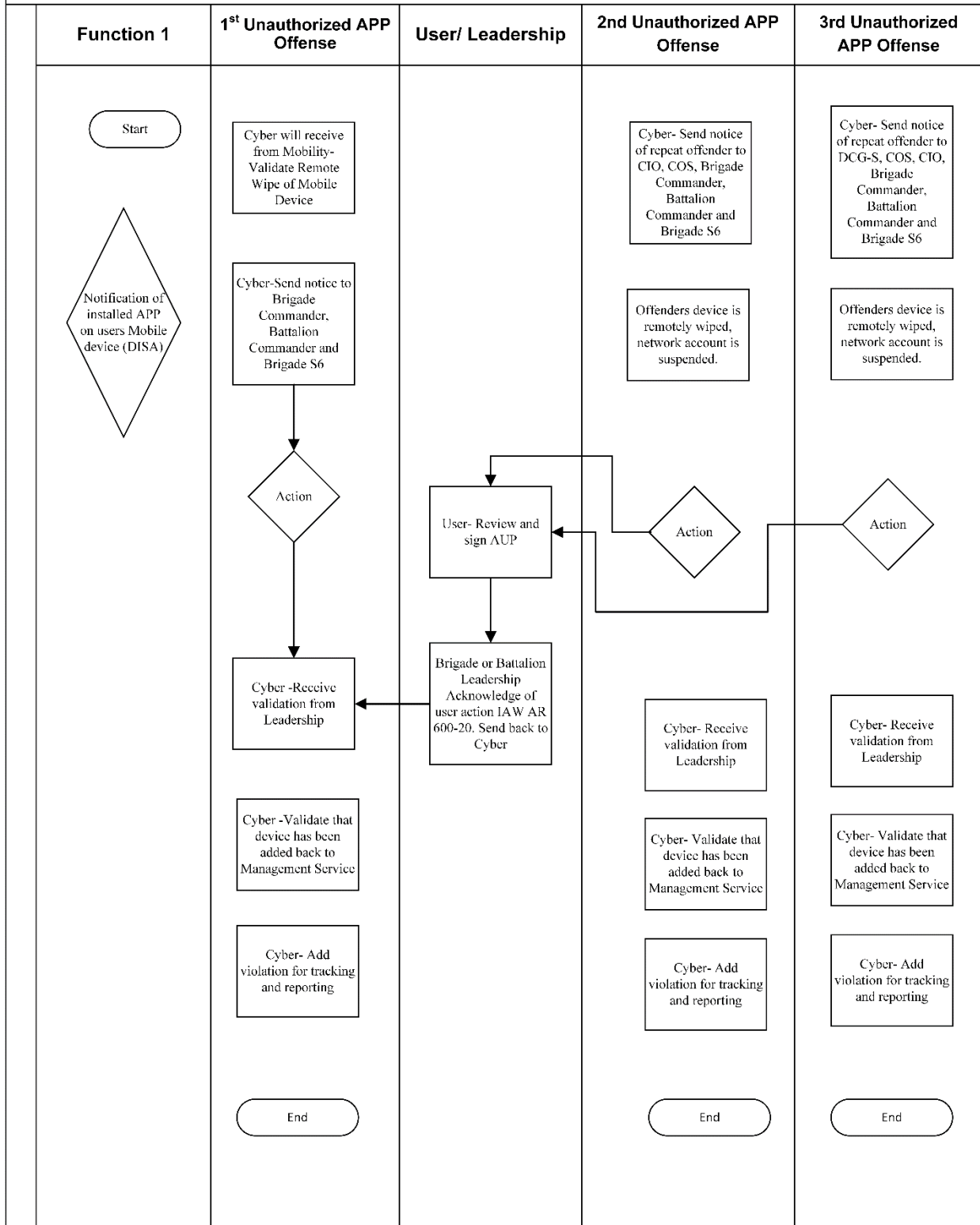
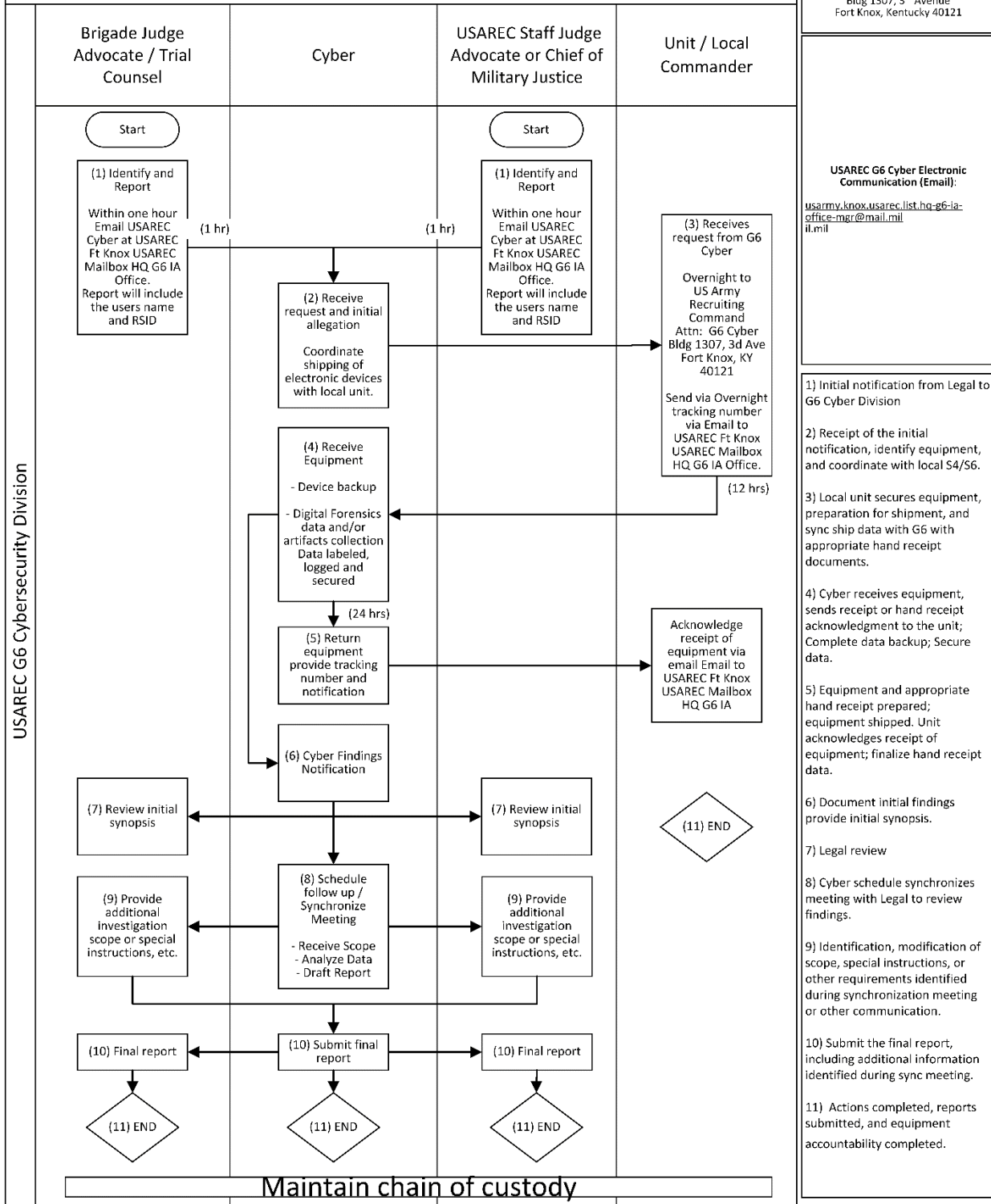


Figure 2-11. Mobile Device Compromise APP Leadership Notification Process

Figure 2-12 Data Retention Process (Investigations)



USAREC G6 Cyber Physical Address:
US Army Recruiting Command
Attn: G6 Cyber Division (CISO)
Bldg 1307, 3rd Avenue
Fort Knox, Kentucky 40121

USAREC G6 Cyber Electronic Communication (Email):
usarmy.knox.usarec.list.hq-g6-ia-office-mgr@mail.mil
il.mil

- 1) Initial notification from Legal to G6 Cyber Division
- 2) Receipt of the initial notification, identify equipment, and coordinate with local S4/S6.
- 3) Local unit secures equipment, preparation for shipment, and sync ship data with G6 with appropriate hand receipt documents.
- 4) Cyber receives equipment, sends receipt or hand receipt acknowledgment to the unit; Complete data backup; Secure data.
- 5) Equipment and appropriate hand receipt prepared; equipment shipped. Unit acknowledges receipt of equipment; finalize hand receipt data.
- 6) Document initial findings provide initial synopsis.
- 7) Legal review
- 8) Cyber schedule synchronizes meeting with Legal to review findings.
- 9) Identification, modification of scope, special instructions, or other requirements identified during synchronization meeting or other communication.
- 10) Submit the final report, including additional information identified during sync meeting.
- 11) Actions completed, reports submitted, and equipment accountability completed.

Figure 2-12. Data Retention Process (Investigations)

Chapter 3.

G-6 Information Technology Business Office.

3-1. Information Technology Business Office (ITBO)

ITBO consists of the IT Resources Branch and the Administrative Services Branch. Both branches have certain roles as they apply to USAREC, the G-6 Directorate, and are listed below.

3-2. IT Resources Branch roles are:

- a. Program Objective Memorandum (POM) plans with G-6 Deputy Director.
- b. Acquisition Management Oversight (AMO) packet processing.
- c. Technology research.
- d. Contract management.
- e. Attendance at contract review boards.
- f. Attend POM build meetings.
- g. DA Form 3953 reviews and processing.
- h. Maintenance of Basis of Issue Plan (BOIP).
- i. Planning, Programming, Budgeting, and Execution Process (PPBE).
- j. Career Program 34 Registration, Outreach and Certification
- k. Proponent for all IT Service Requests.

3-3. Information Technology Business Office roles are:

- a. Publications management and Publications Control Officer (PCO) duties.
- b. Forms Management and Forms Management Officer (FMO) duties.
- c. USAREC business card program.
- d. Dynamic publications and PDF fillable forms.
- e. G-6 Print Management and Print Management Officer duties.
- f. Manages DA/DOD higher level publications/forms accounts through the St. Louis Publication warehouse.
- g. FOIA/Privacy Act programs.
- h. Request records from proponent within USAREC.
- i. Redact records supporting FOIA/PA record requests.
- j. Advises the G-6 on matters dealing with Freedom of Information Act requests.
- k. Process requests under Privacy Act.

3-4. Information Technology Business Office Division Business Processes.

- a. Information Technology Business Office (see figure 3-1).
- b. Information Technology Business Office Process (see figure 3-2).
- c. Asset Replacement Process (see figure 3-3).
- d. ITEPS Service Request Process (see figure 3-4).
- e. Publications Revision Process (see Figure 3-5)
- f. Business Card Request Process (see Figure 3-6)
- g. Freedom of Information Act Process (FOIA/Privacy Act). (See Figure 3-7)
- h. CP-34 Registration Process (see Figure 3-8)
- i. CP-34 Outreach Process (see Figure 3-9)
- j. CP-34 Certification Process (see Figure 3-10)

Figure 3-1. ITBO

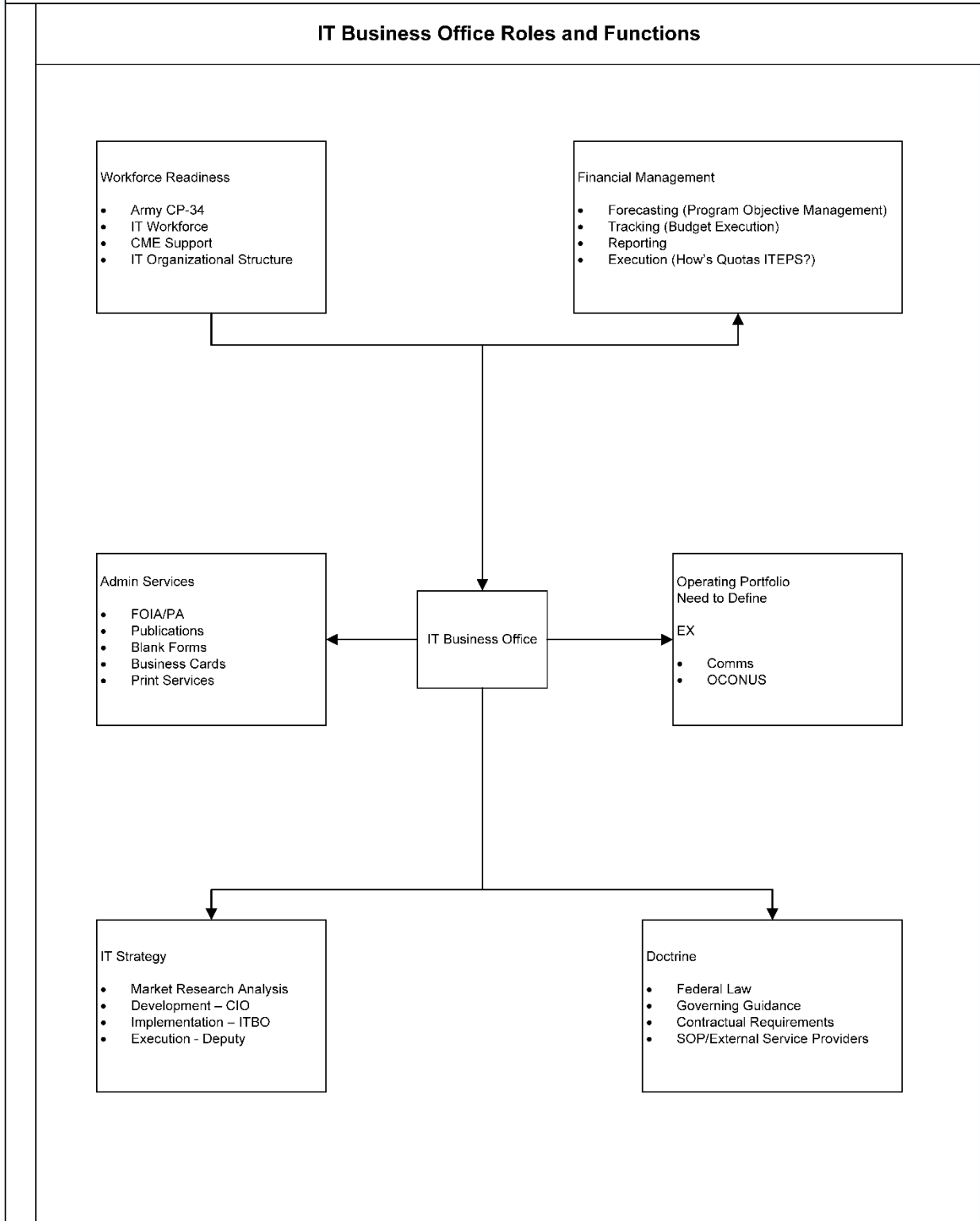


Figure 3-1. ITBO Roles and Responsibilities

Figure 3-2. ITBO Business Process

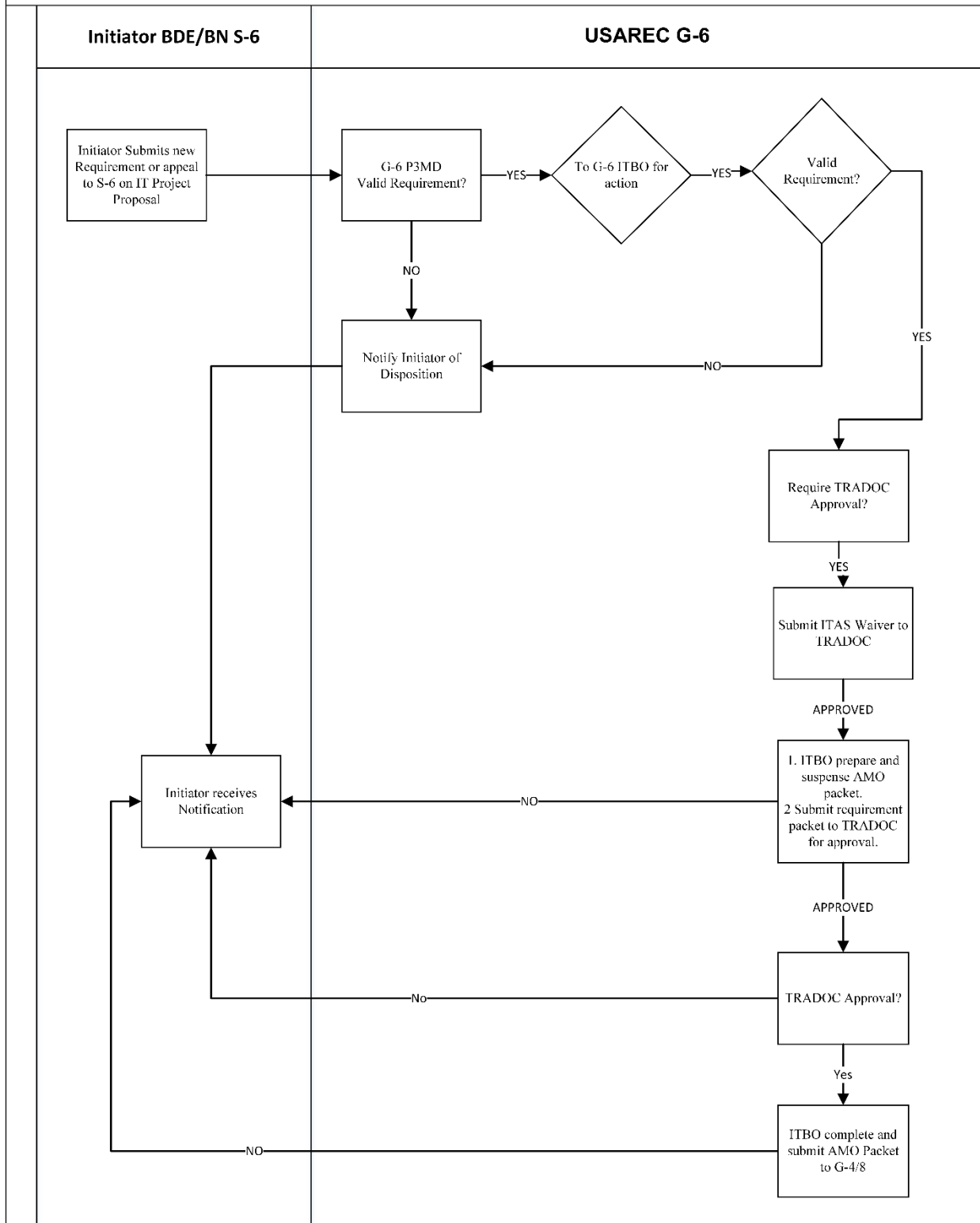


Figure 3-2. ITBO Business Process

Figure 3-3. Asset Replacement Process

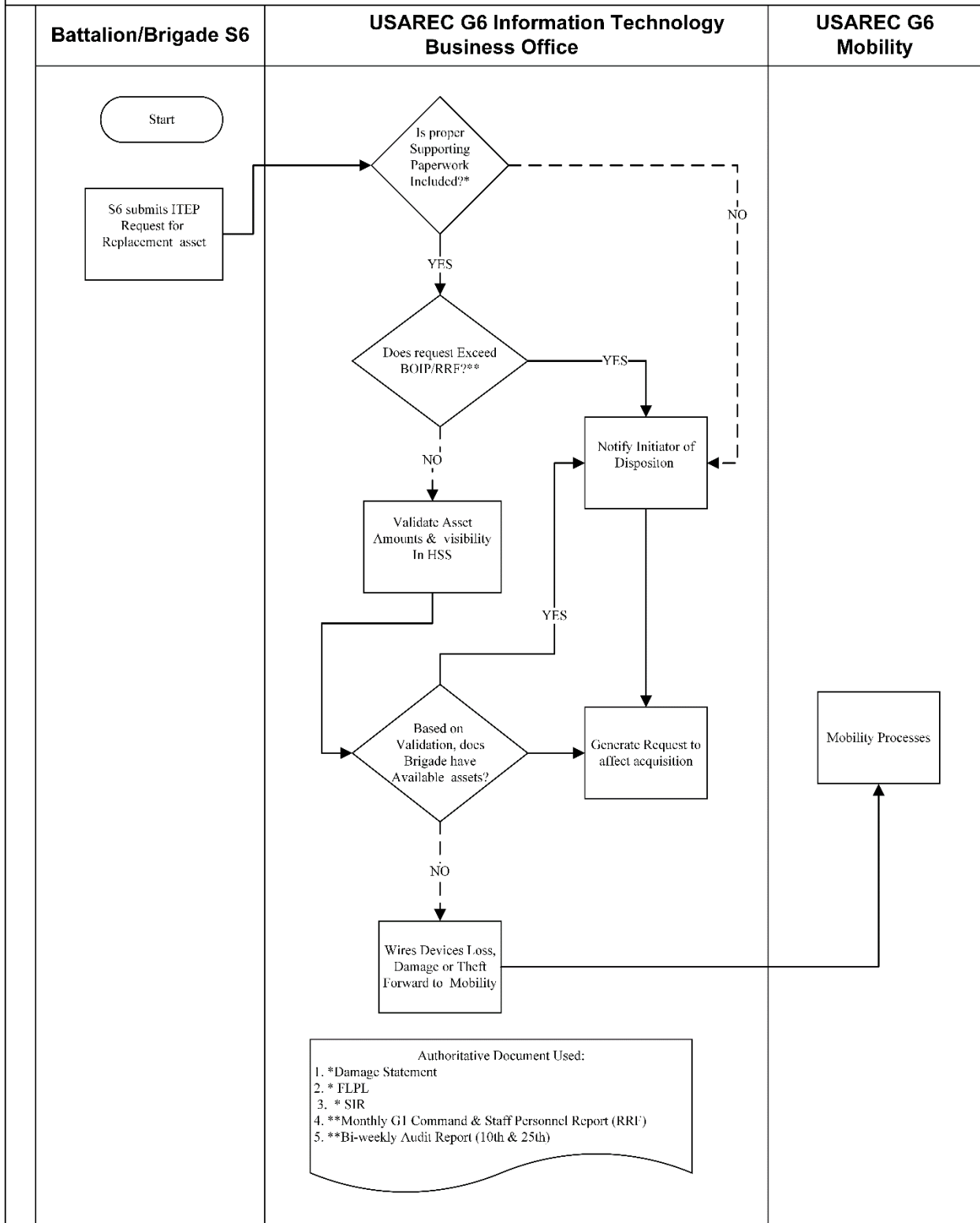


Figure 3-3. Asset Replacement Process

Figure 3-4. ITEPS Service Request Process (IT Equipment, Products & Services)

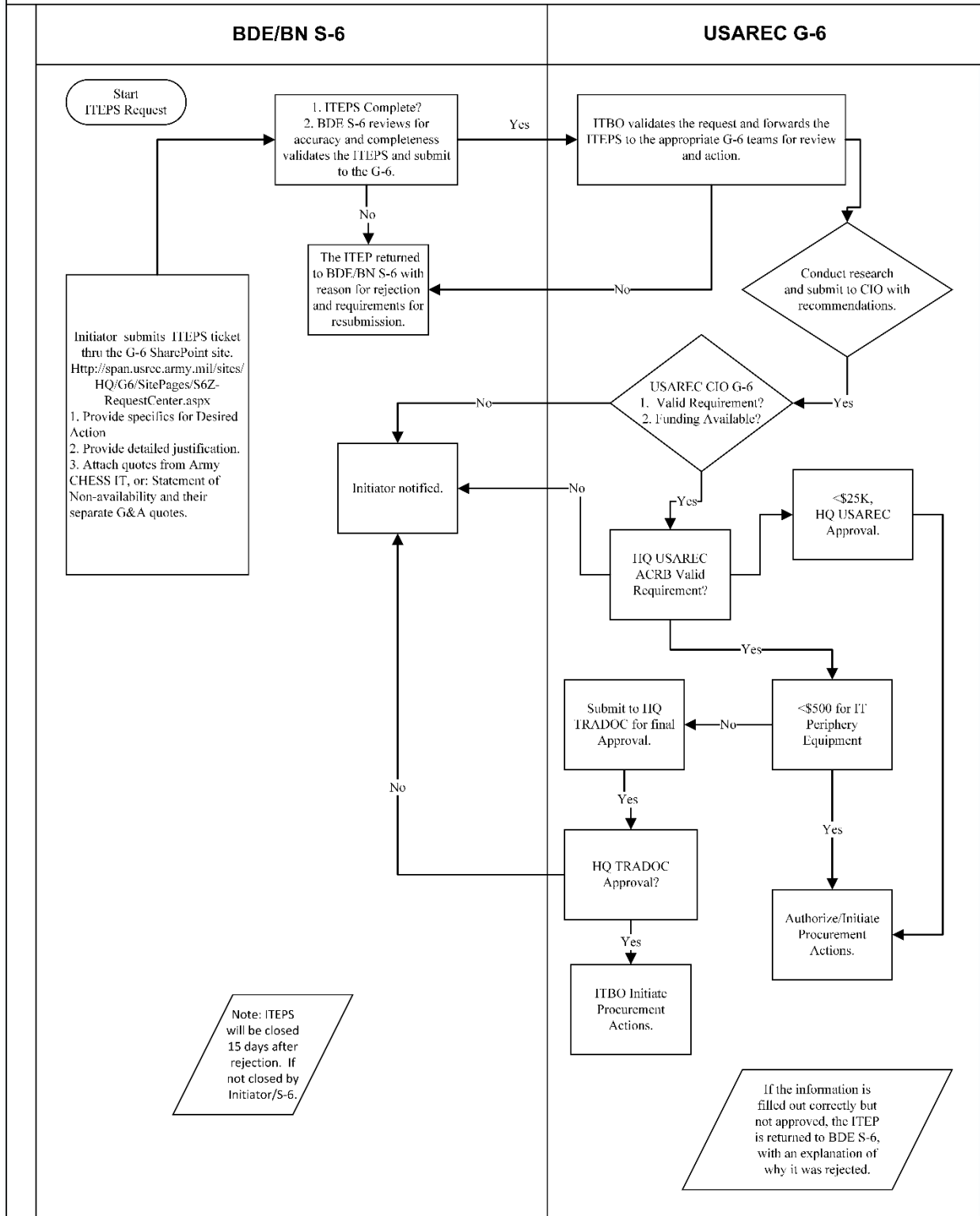


Figure 3-4. ITEPS Service Request Process

Figure 3-5. New, Revision, or Rescind Publication Process

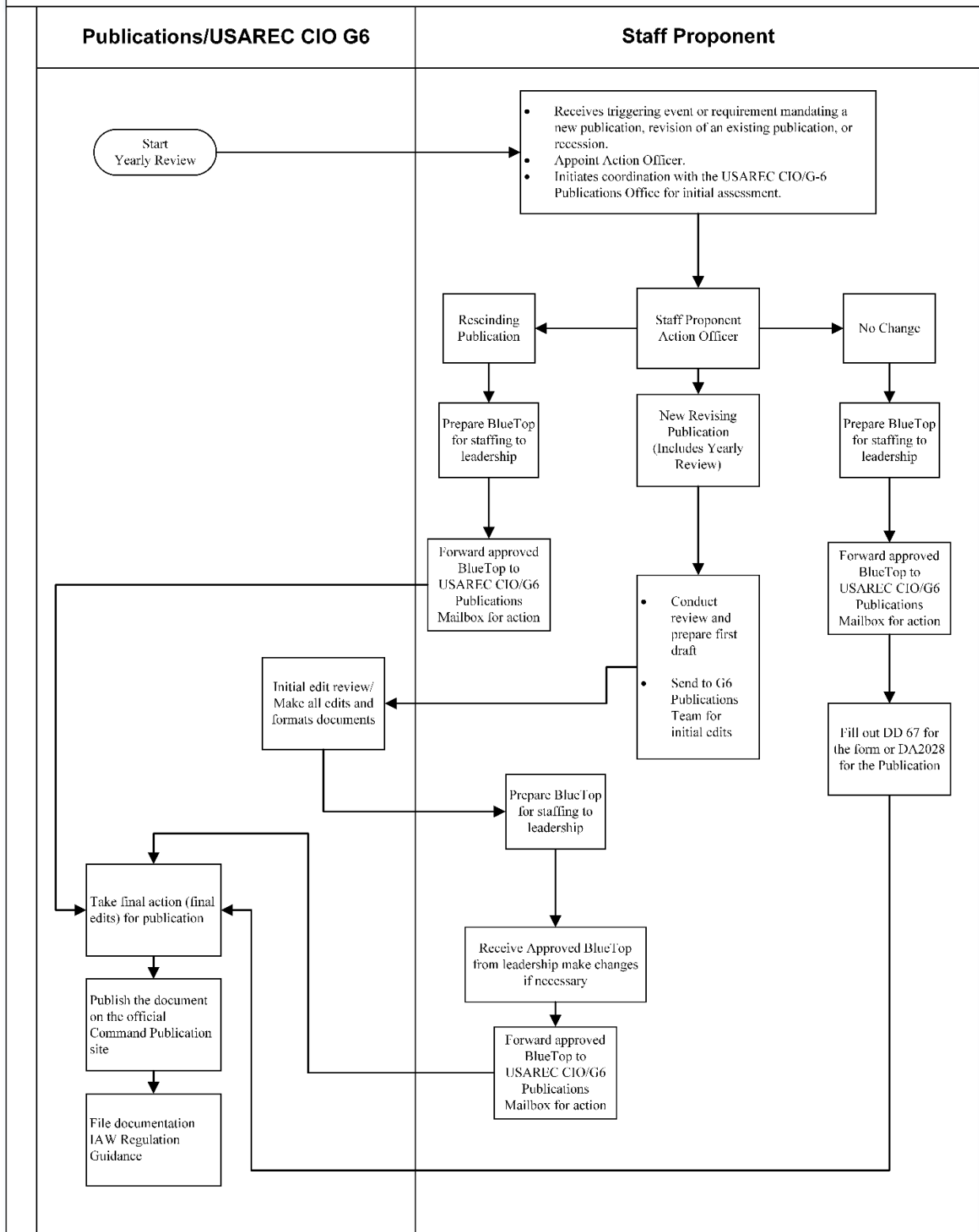


Figure 3-5. New, Revision, or Rescind Publication Process

Figure 3-6. Business Card Request Process

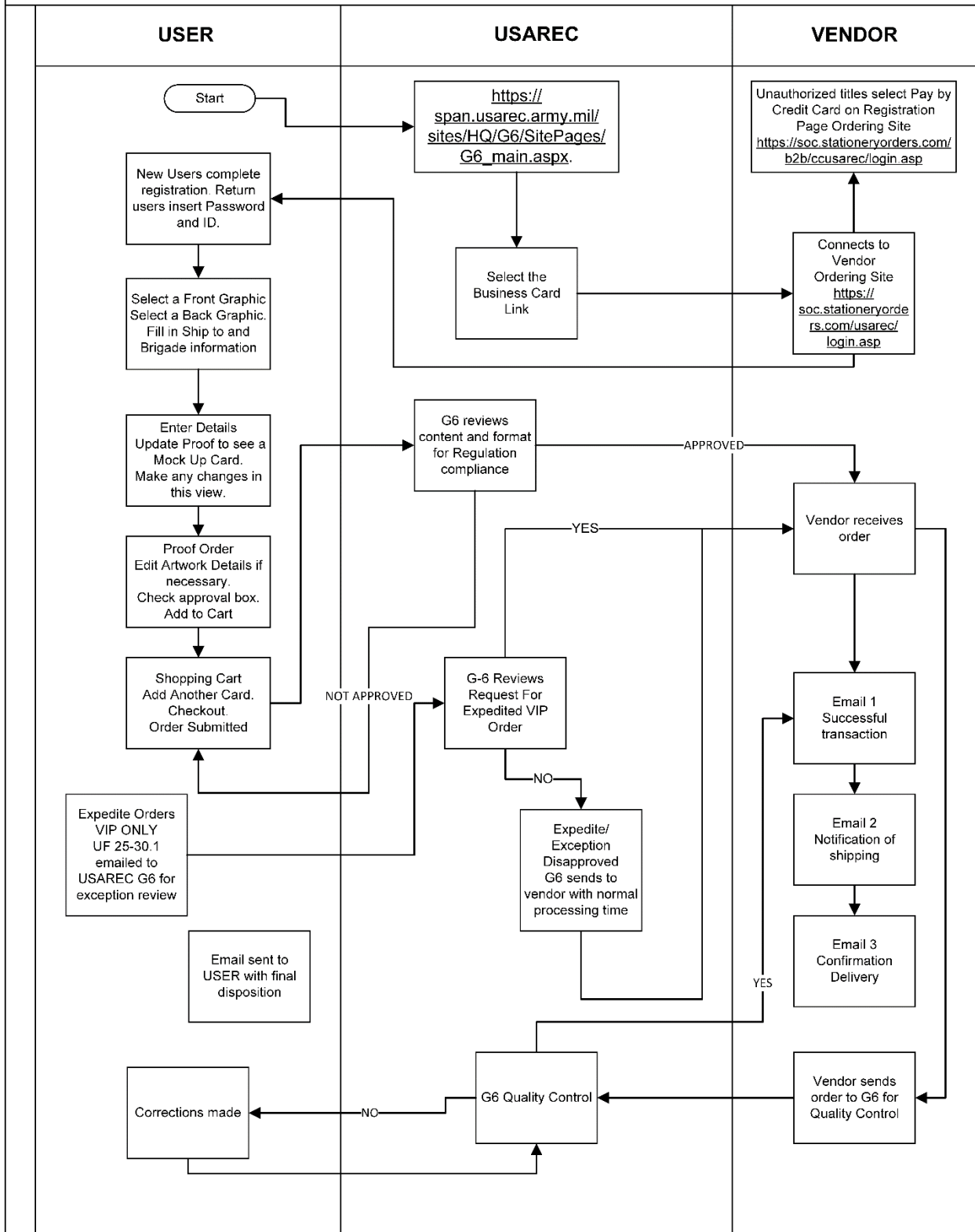


Figure 3-6. Business Card Request Process

Figure 3-7. Freedom of Information Act (FOIA)/Privacy Act Process

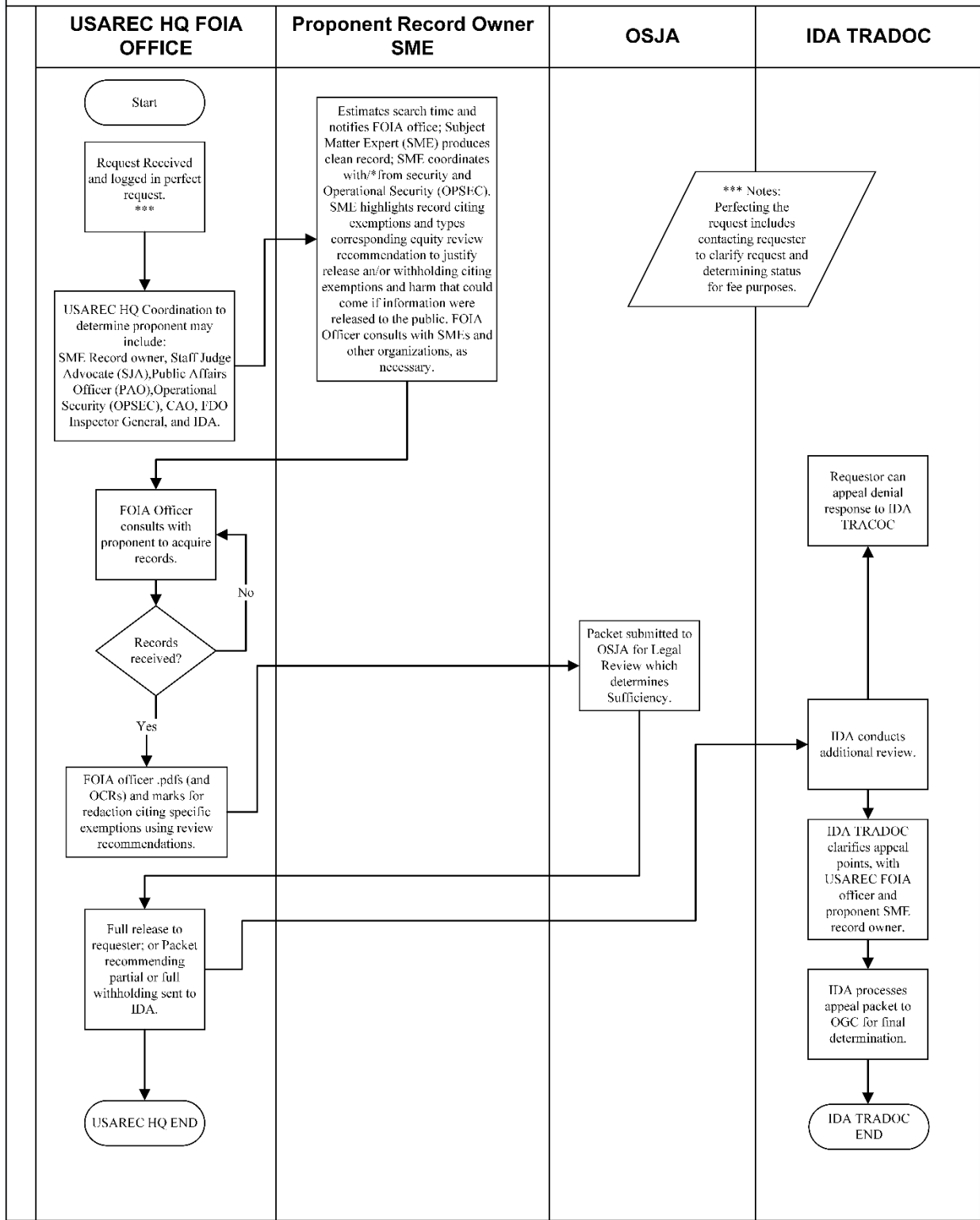


Figure 3-7. Freedom of Information Act Process

Figure 3-8. CP-34 Registration

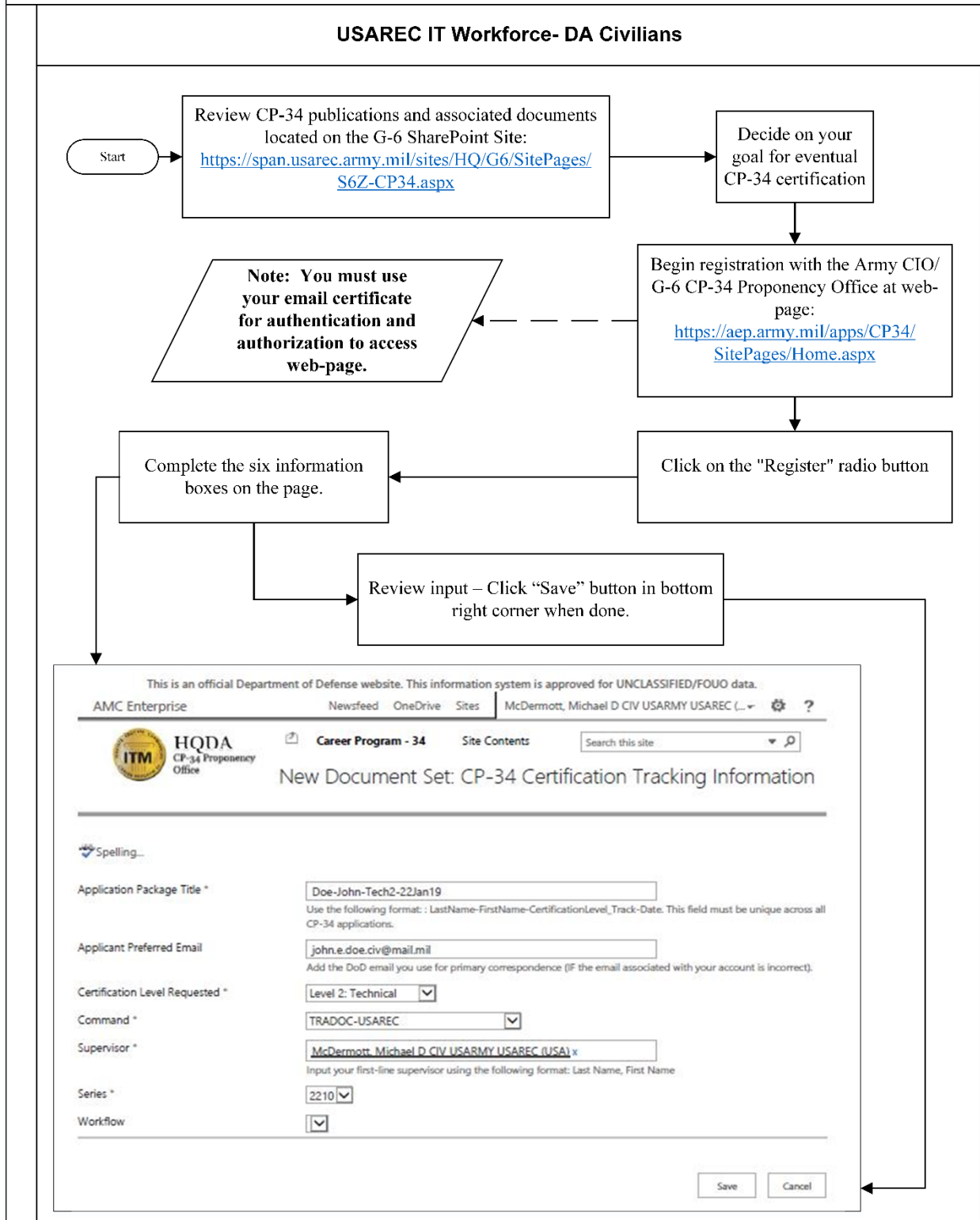


Figure 3-8. CP-34 Registration Process

Figure 3-9. CP-34 Certification Process

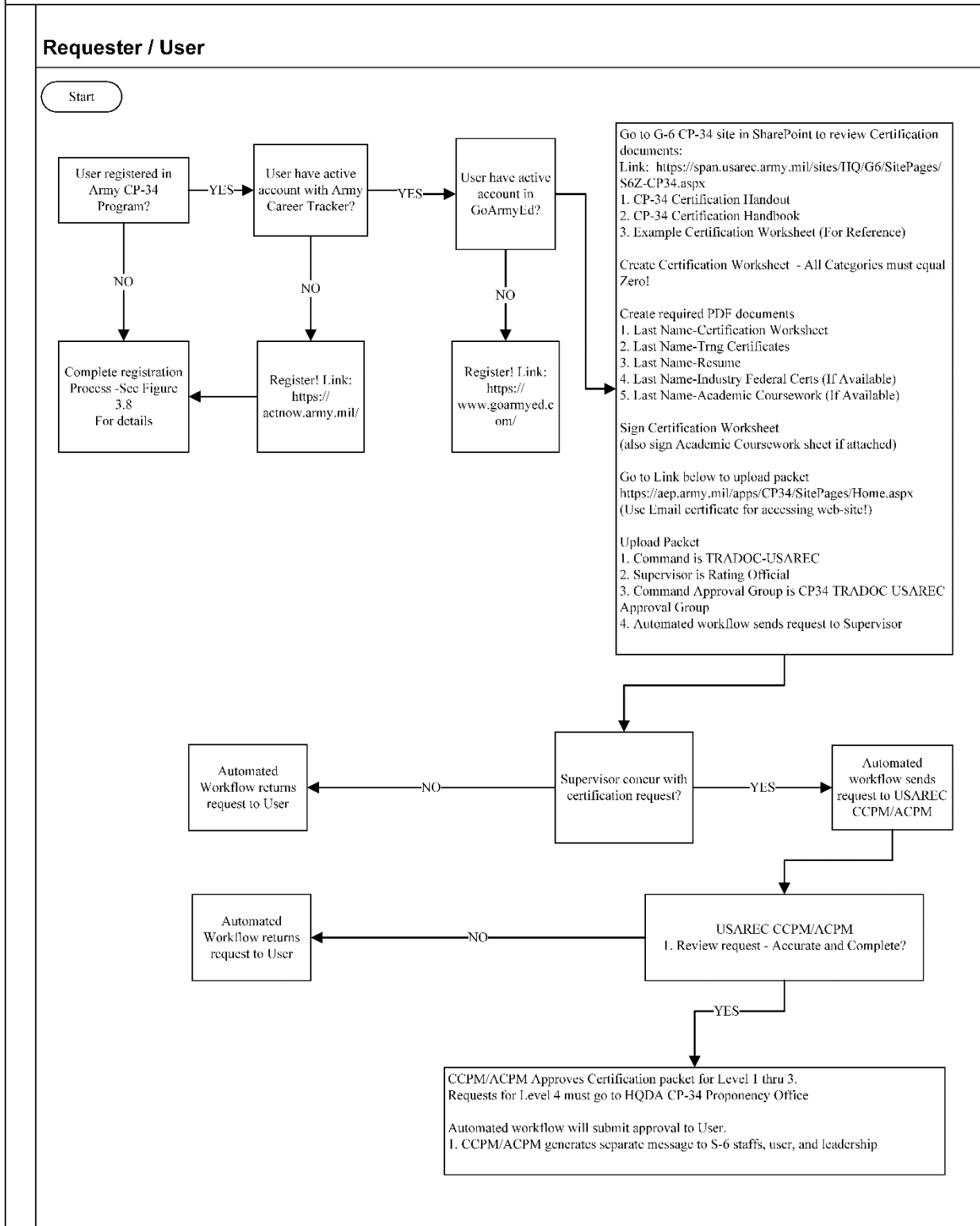


Figure 3-9. CP-34 Outreach Process

Figure 3-10. CP-34 Outreach Training Request Process

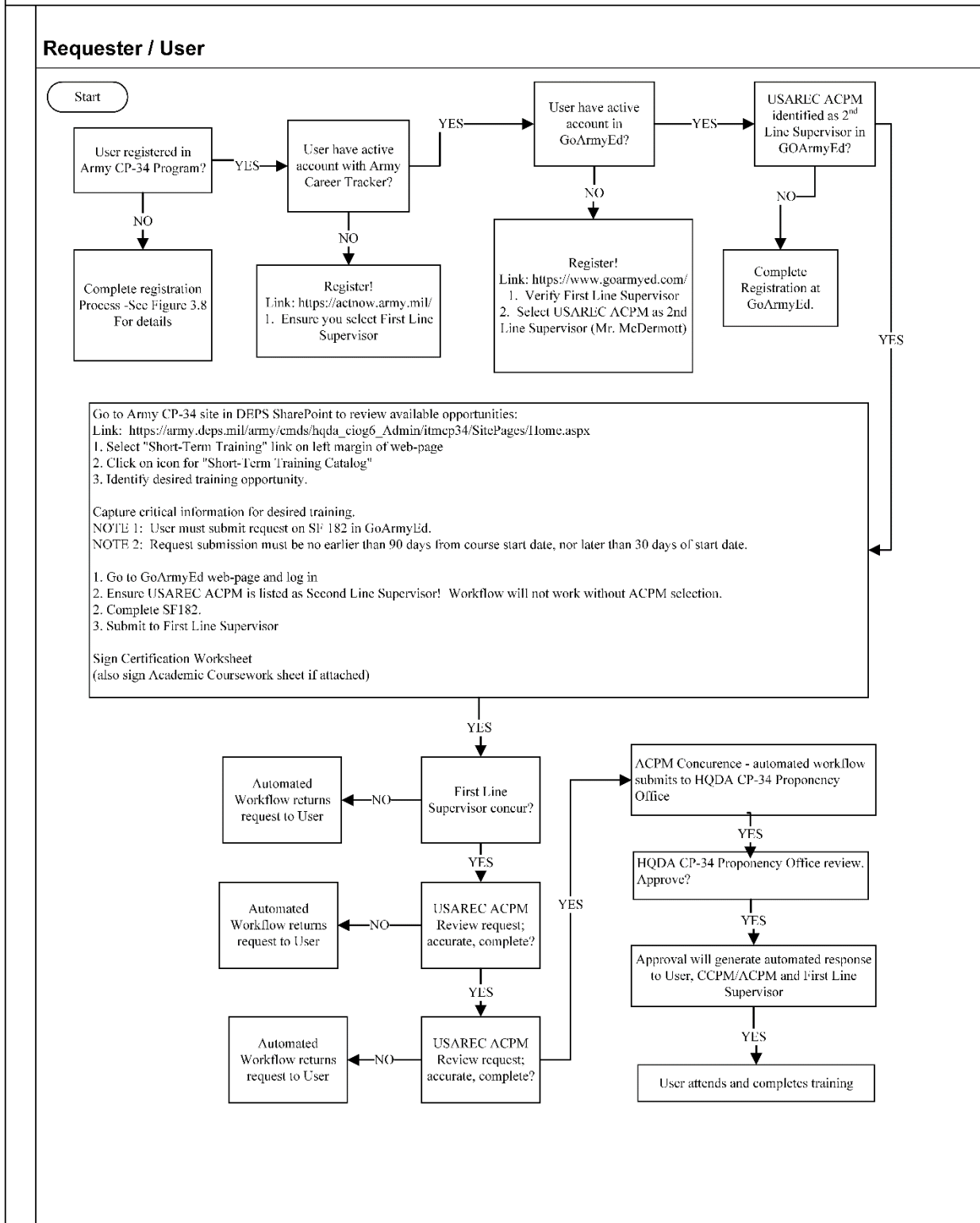


Figure 3-10. CP-34 Certification Program Process

Chapter 4.

G-6 Operations Division Roles and Business Processes.

4-1. The Operations Division

Operation Division consists of the Network Operations Branch and IT Plans Branch.

4-2. Network Operations Branch roles are:

- a. Network performance monitoring and reporting.
- b. Maintenance schedules.
- c. Network operations synchronization with service providers.
- d. All internal and external G-6 tasks.
- e. Prepare and Post Critical Information Alerts.
- f. Attend daily service provider briefings.
- g. Report Network outages.
- h. Calendar for maintenance.
- i. Monthly maintenance calendar planning meetings.

4-3. IT Plans Branch roles are:

- a. Operations orders.
- b. Trip book preparations.
- c. Positioning, Analysis, and Evaluation (PAE) planning and coordination.
- d. Attendance at G-3 operational planning cell meetings.
- e. BDE Operations Update Assessment reviews and preparation of response/status.
- f. S-6 Brown bag training.
- g. G-6 Leadership training.
- h. Mission and vision.
- i. Needs assessment and staff development.
- j. Attend weekly PAE meetings.
- k. Attend monthly G-4 sync meetings.
- l. G-6 expendable tracker.
- m. New solutions for FY lifecycle hardware.
- n. Analyze and assess command technology needs.
- o. Research emerging technology.
- p. Voice Telecommunications Systems (Sustainment and Modernization).
- q. Frame research insights through deliverables.
- r. SOP and Best Business Practices.

4-4. Operations Division Business

Operations Division Business Processes are listed below.

- a. Internal Task Initiation and Tracking Process. (See Figure 4-1)
- b. USAREC Telephone/RFS Process Flow (see Figure 4-2)

Figure 4-1. Internal Task Initiation and Tracking Process

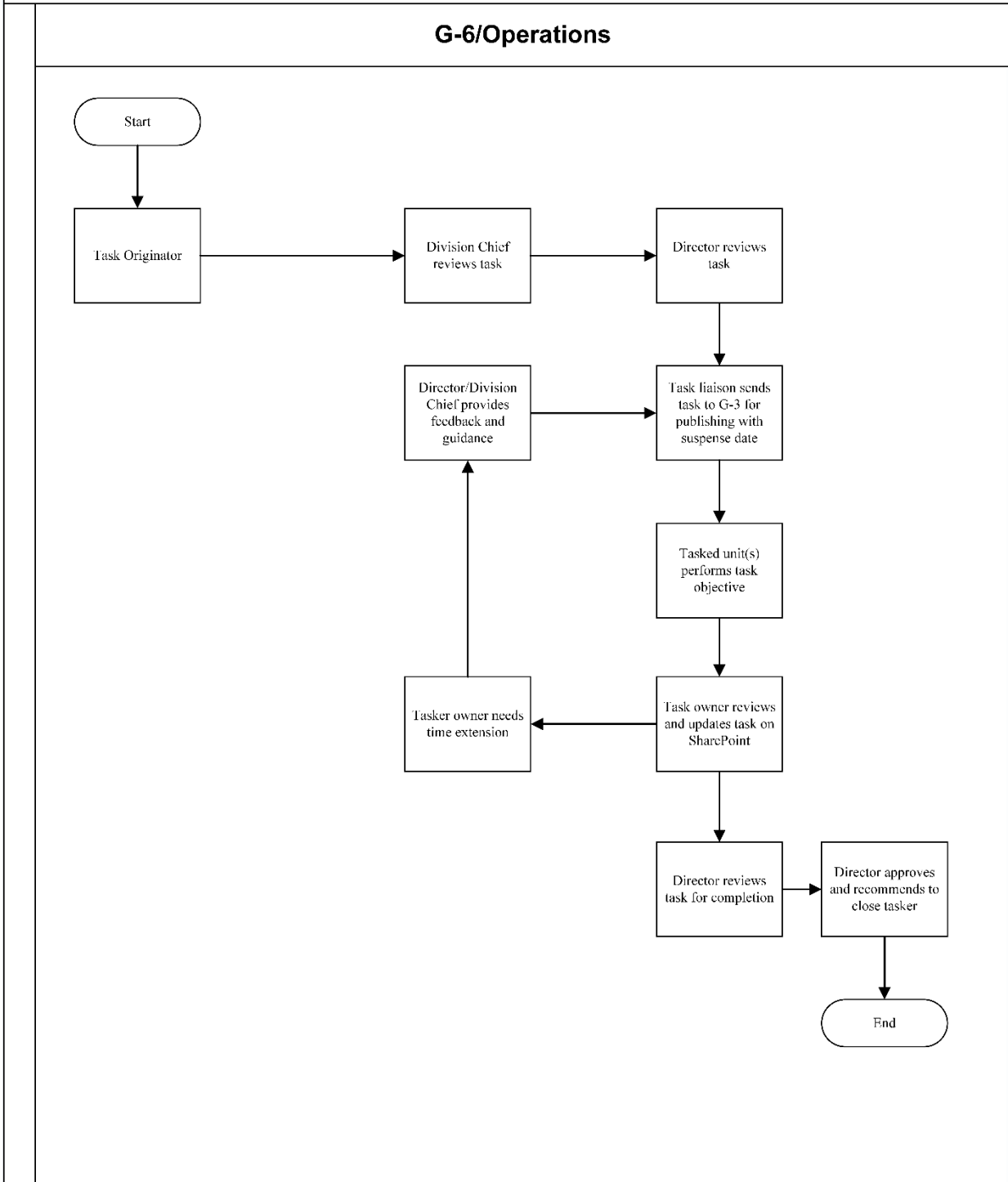


Figure 4-1. Internal Task Initiation and Tracking Process

Figure 4-2. USAREC Telecom/RFS process flow (Includes new and replacement telephones)

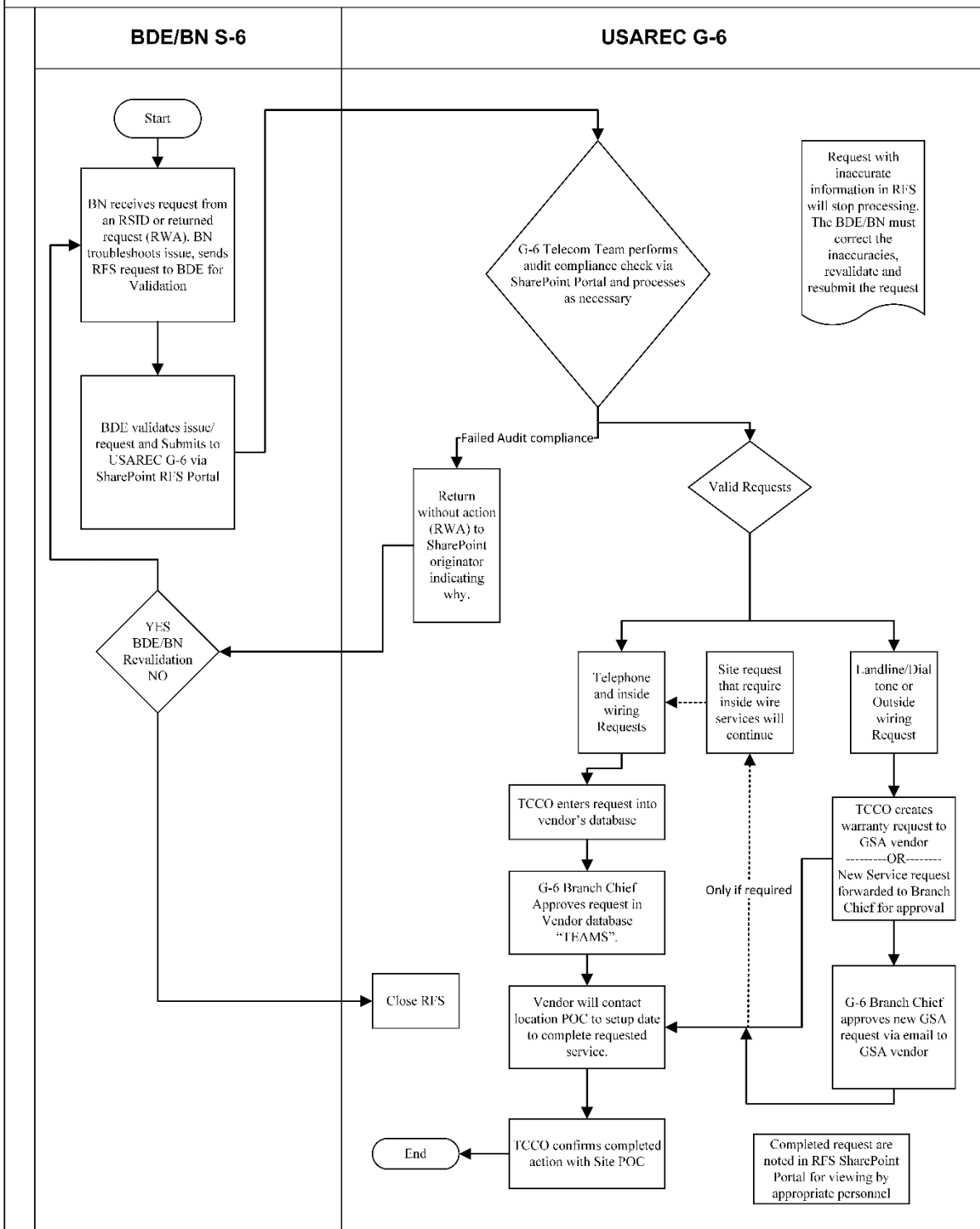


Figure 4-2. USAREC Telecom/RFS Process Flow (Includes new and Replacement Telephones)

Chapter 5.

G-6 Integrated Solutions Division

5-1. Integrated Solutions Division

Integrated Solutions Division Business processes are listed below:

- a. Mobility Ticket Process. (See Figure 5-1)
- b. MobileIron Process. (See Figure 5-2)
- c. Live Scan Fingerprint Request Process (see Figure 5-3)
- d. Mobile Support Request (User) Process (see Figure 5-4)
- e. Command Mobility Device Disposition Process (see Figure 5-5)
- f. LiveScan Device Warranty Replacement Process (see Figure 5-6)
- g. Offline Device Enrollment-Chess Software Request Process (see Figure 5-7)
- h. Offline Device Enrollment –MaaS360 Process (see Figure 5-8)
- i. Video Teleconference Request Process (see Figure 5-9)
- j. Software Center Quick Start Guide for Recruiters (see Figure 5-10)
- k. HQ IT Support Request Process (see Figure 5-11)

5-2. IPAD DRMO process:

a. DMUC CMD must be sanitized (factory data reset) before they are transferred to another user or turned in for disposition, see Table 1. This is performed by the user or local Tier 1 and is the responsibility of the owning organization.

b. Supply activities responsible for turning in CMD to Defense Logistics Agency (DLA) disposition Services (aka DRMO) may use the coding in Table 1 to assist in completing the required paperwork (DD Form 1348-1A).

c. The device can be factory reset by you and turned in to DRMO through normal turn in procedures. iPads are treated just like smartphones.

Figure 5-1 Mobility Ticket Process

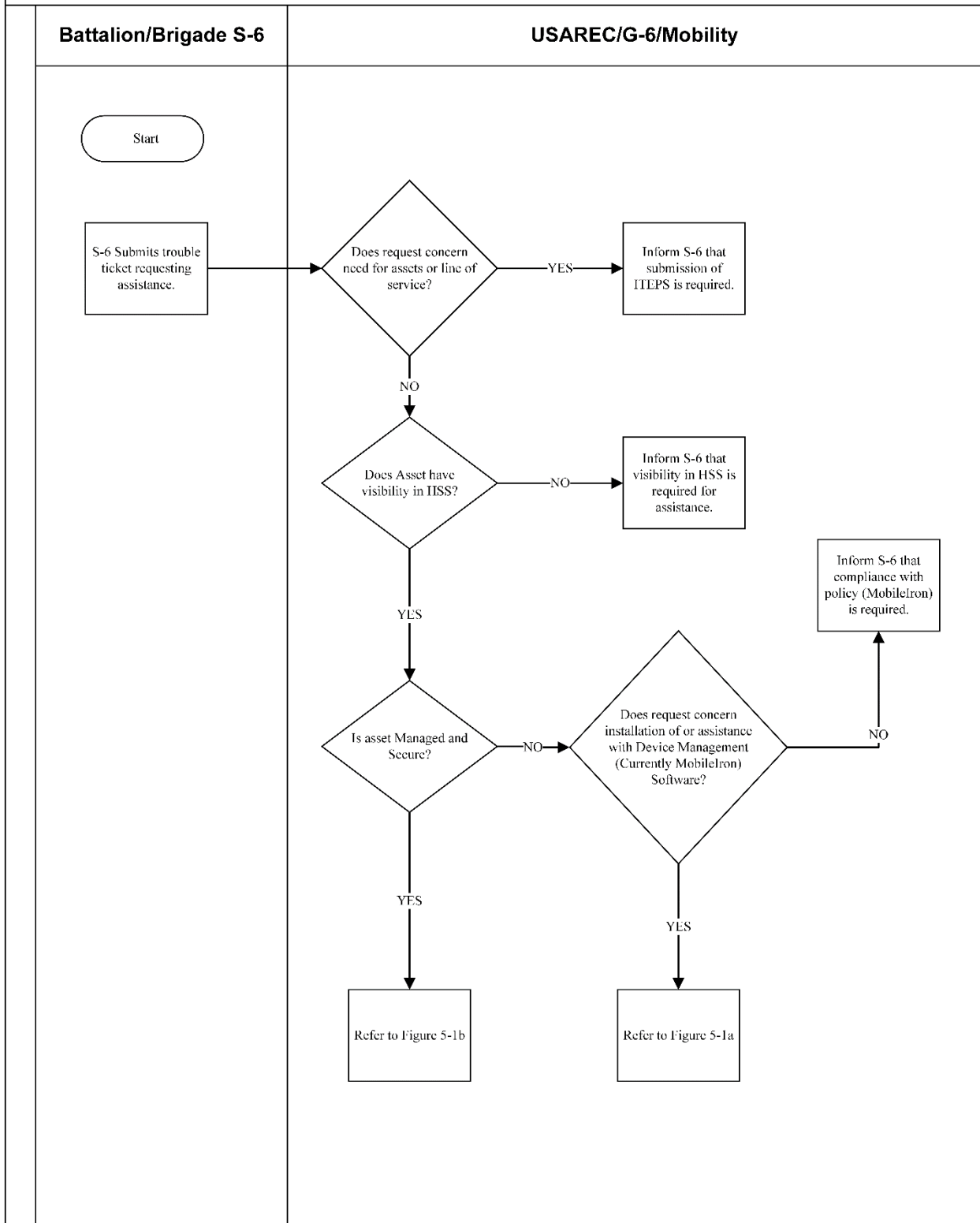


Figure 5-1. Mobility Ticket Process

Figure 5-2 MobileIron Process

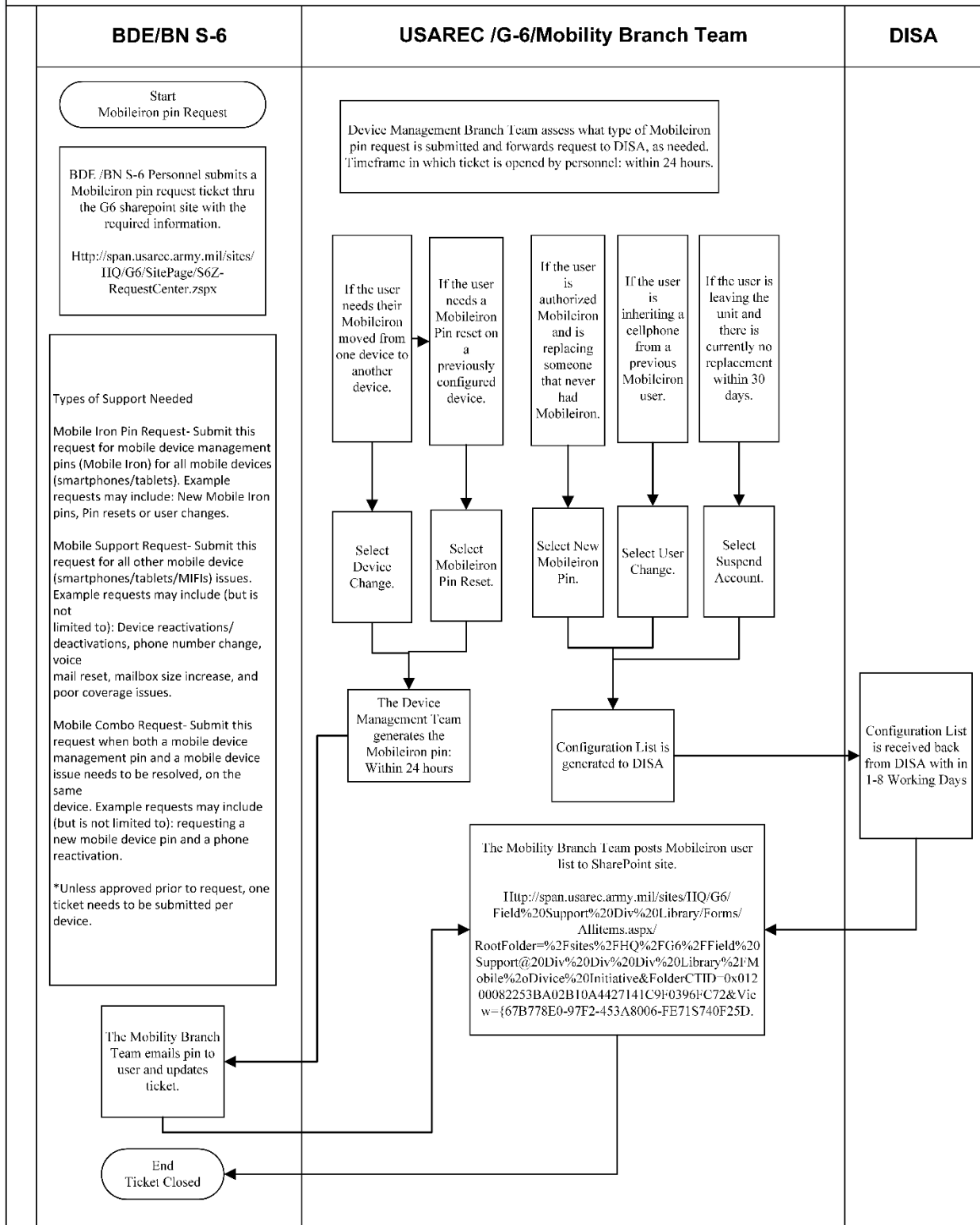


Figure 5-2. MobileIron Process

Figure 5-3 Live Scan Fingerprint Request Process

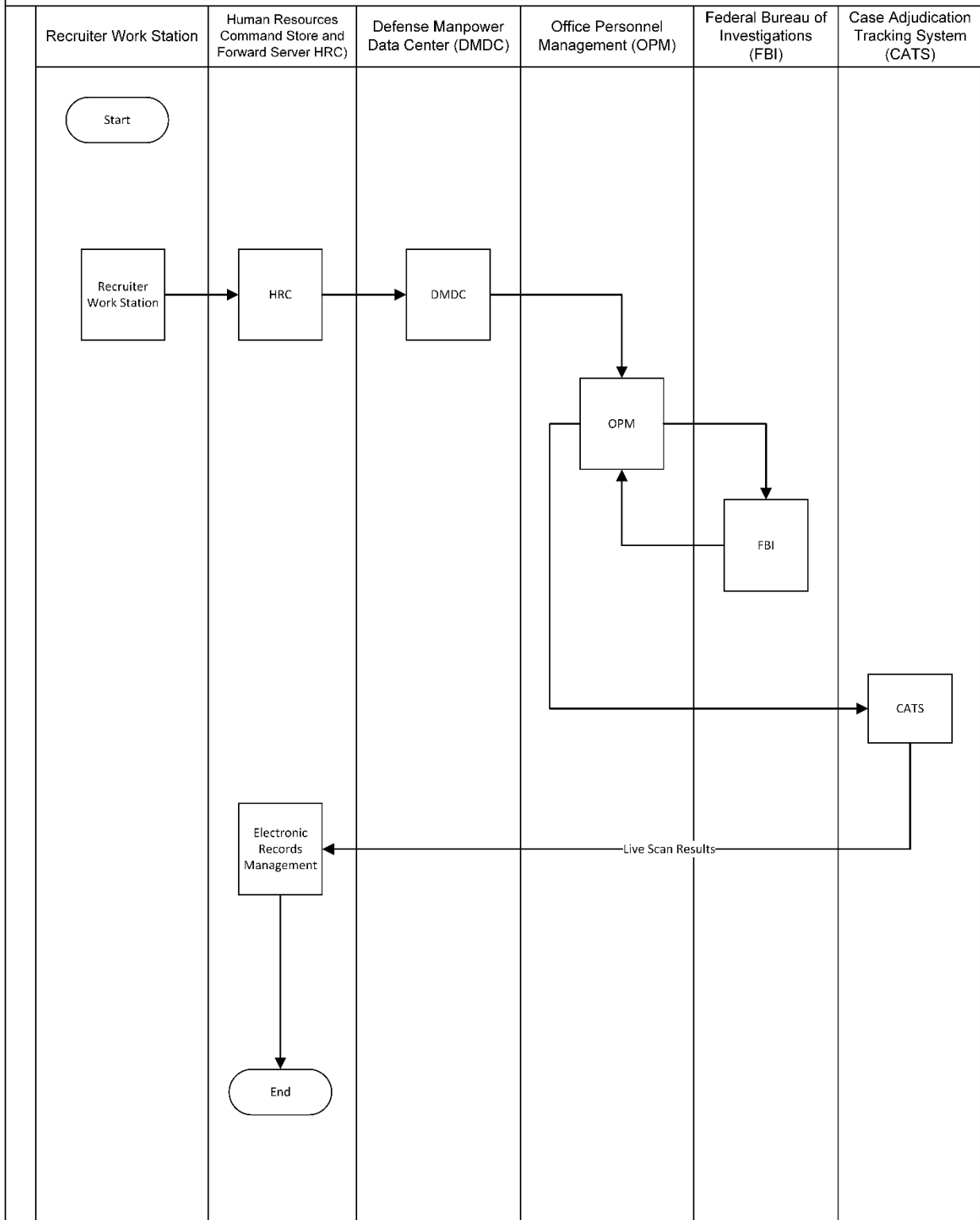


Figure 5-3. LiveScan Device Warranty Replacement Process

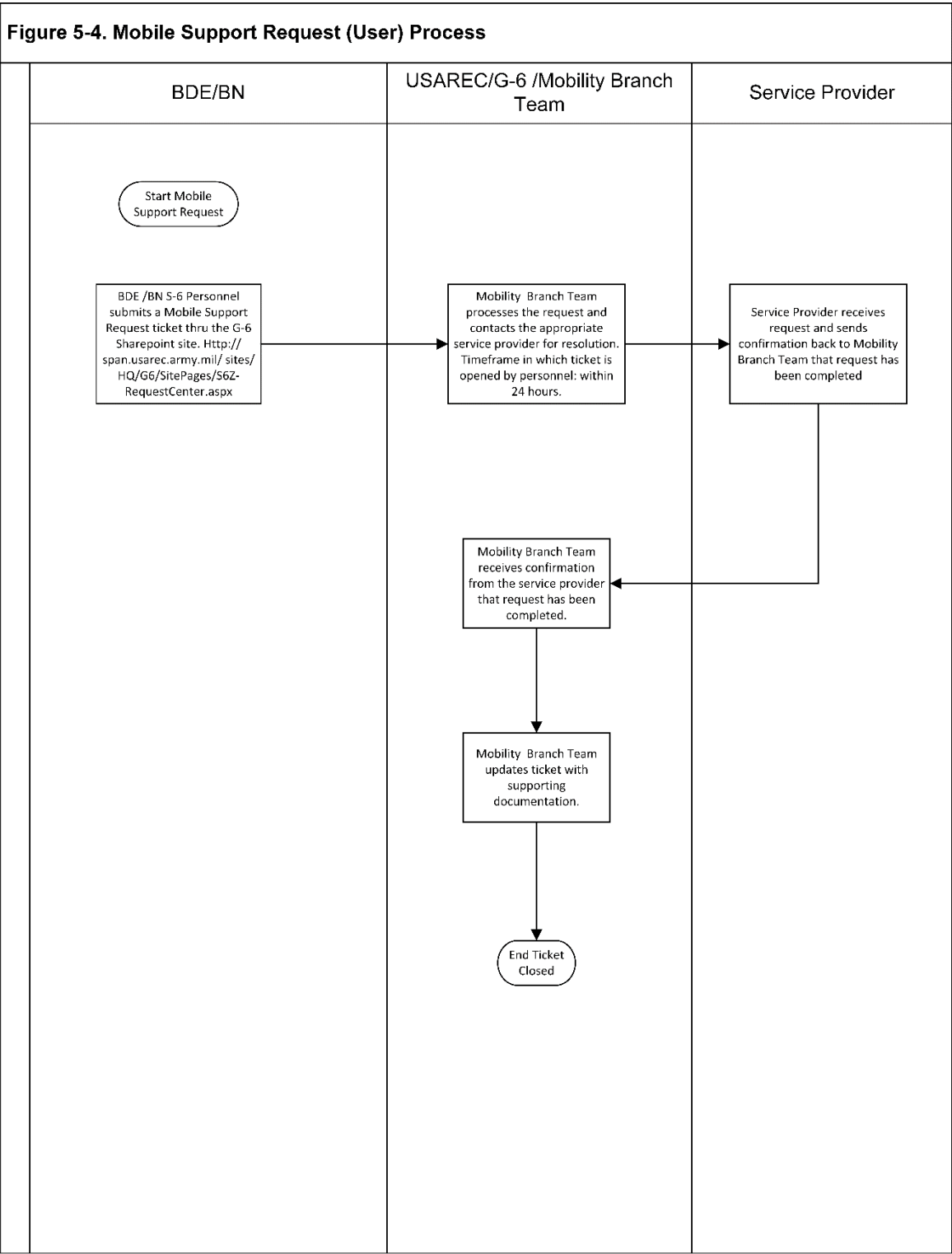


Figure 5-4. Mobile Support Request (USER) Process

Figure 5-5 Command Mobility Device Disposition Process

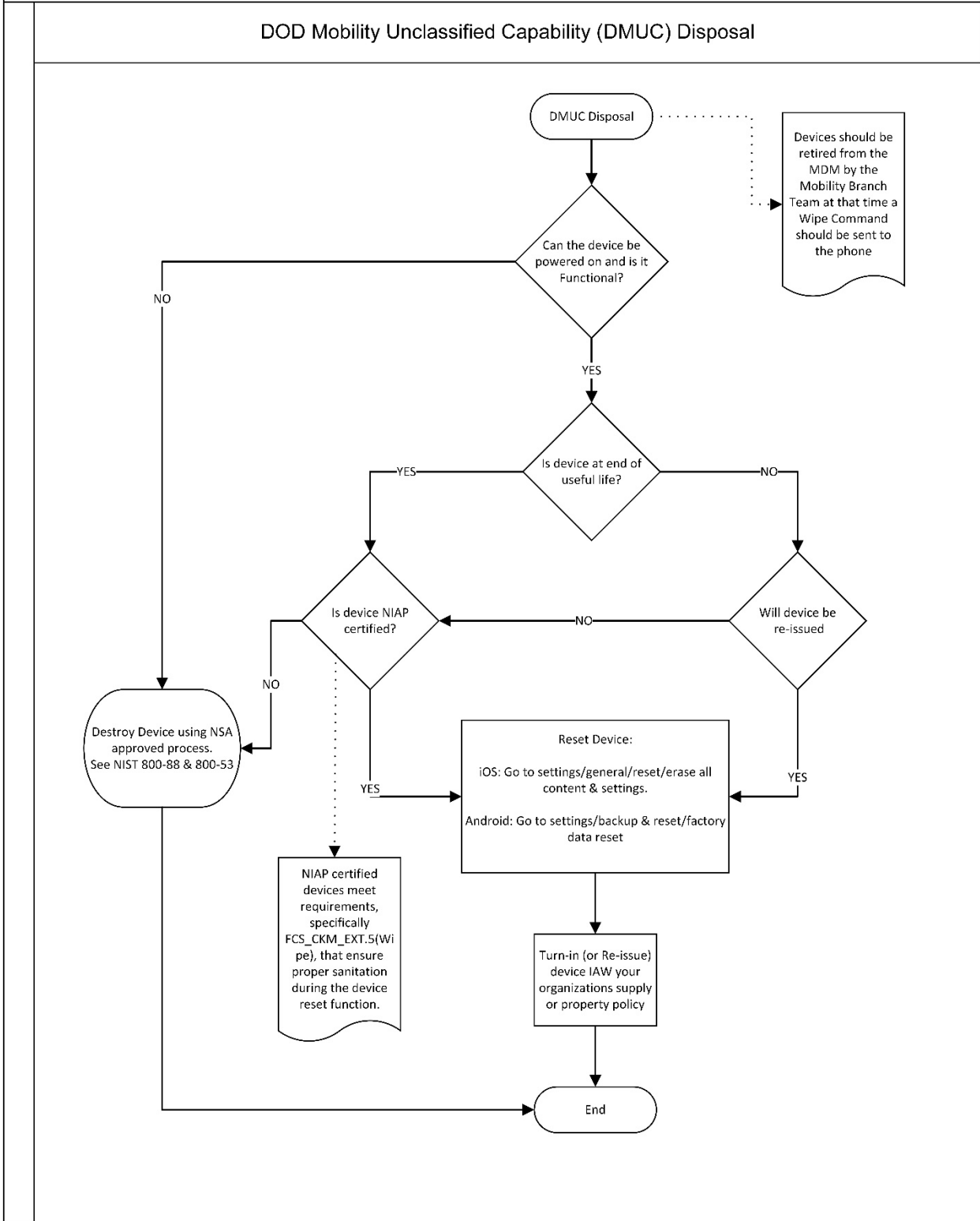


Figure 5-5. Command Mobility Device Disposition Process

Figure 5-6 LiveScan Device Warranty Replacement Process

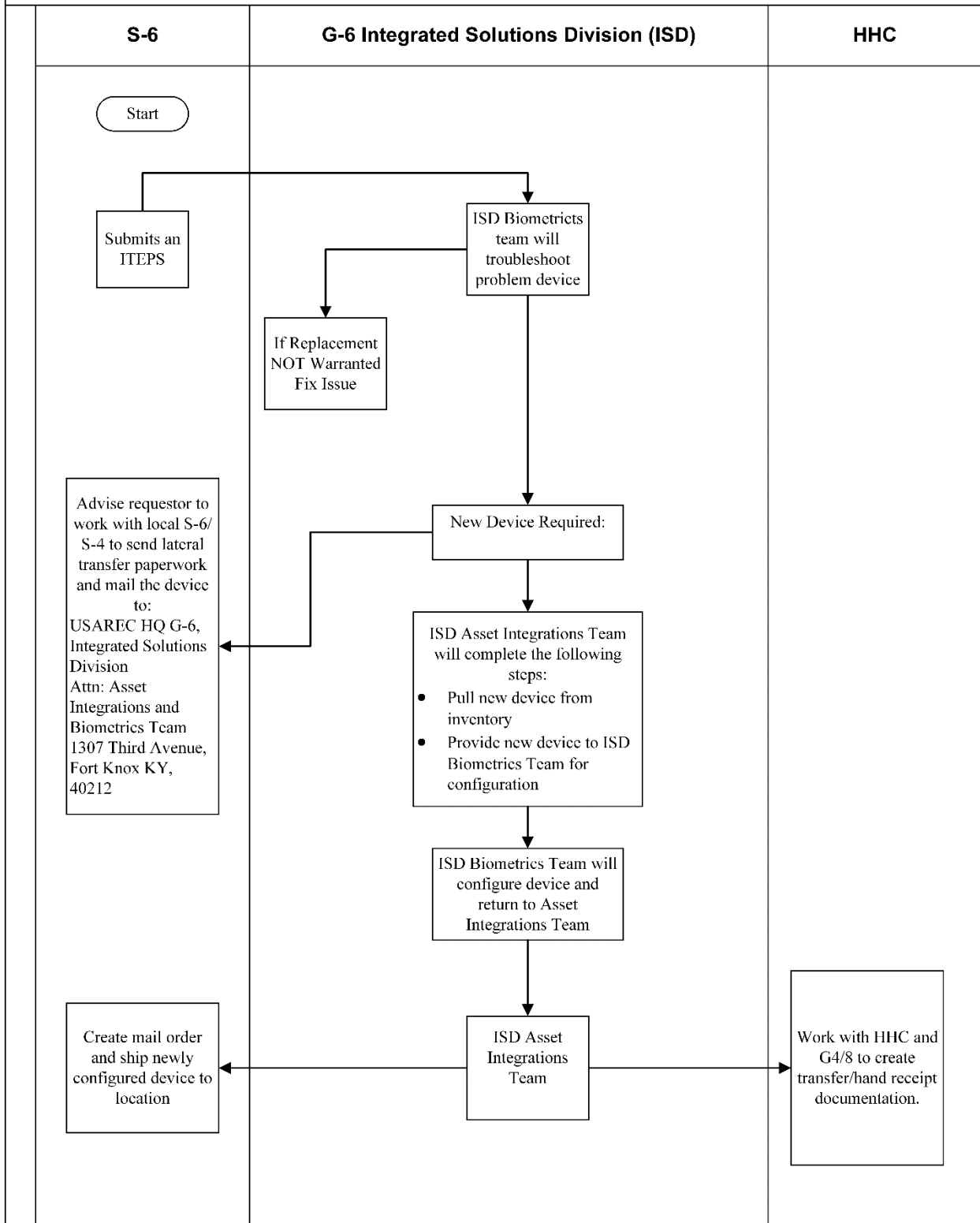


Figure 5-6. LiveScan Device Warranty Replacement Process

Figure 5-7. Offline Device Enrollment-CHES Software Request Process

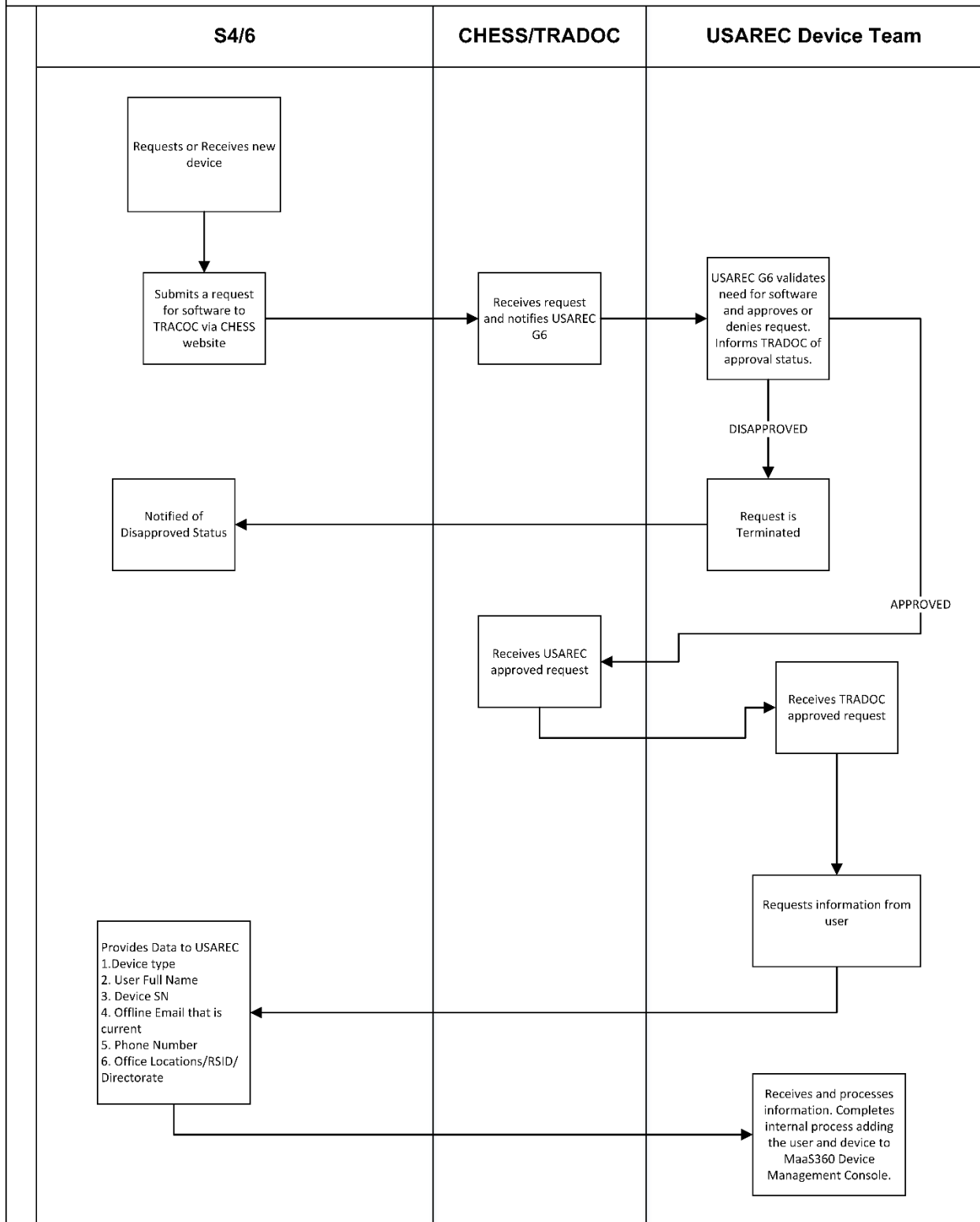


Figure 5-7. Offline Device Enrollment Chess Software Request Process

Figure 5-8. Offline Device Enrollment-MaaS360 Process

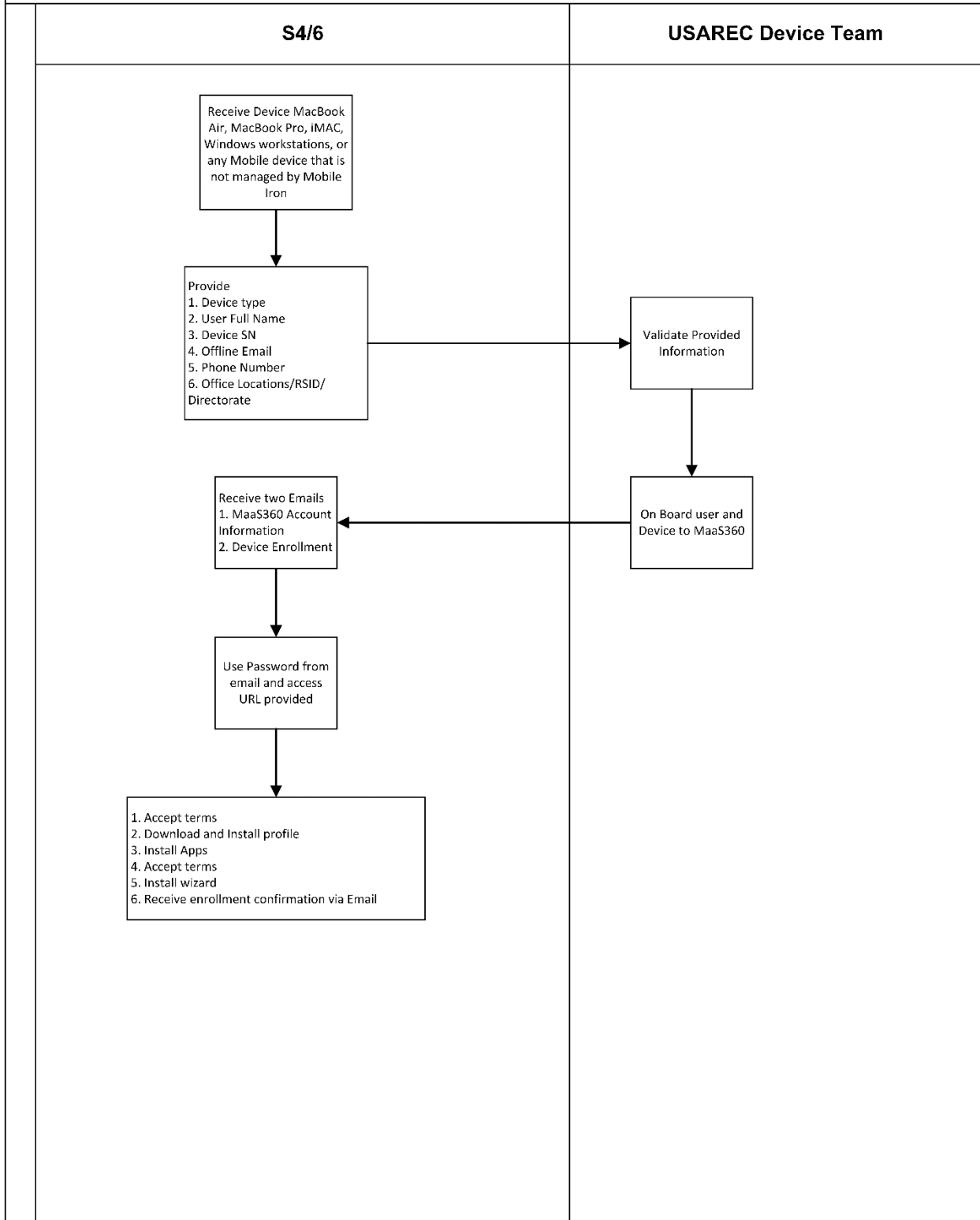


Figure 5-8. Offline Device Enrollment MaaS360 Process

Figure 5-9. Video Teleconference Request Process

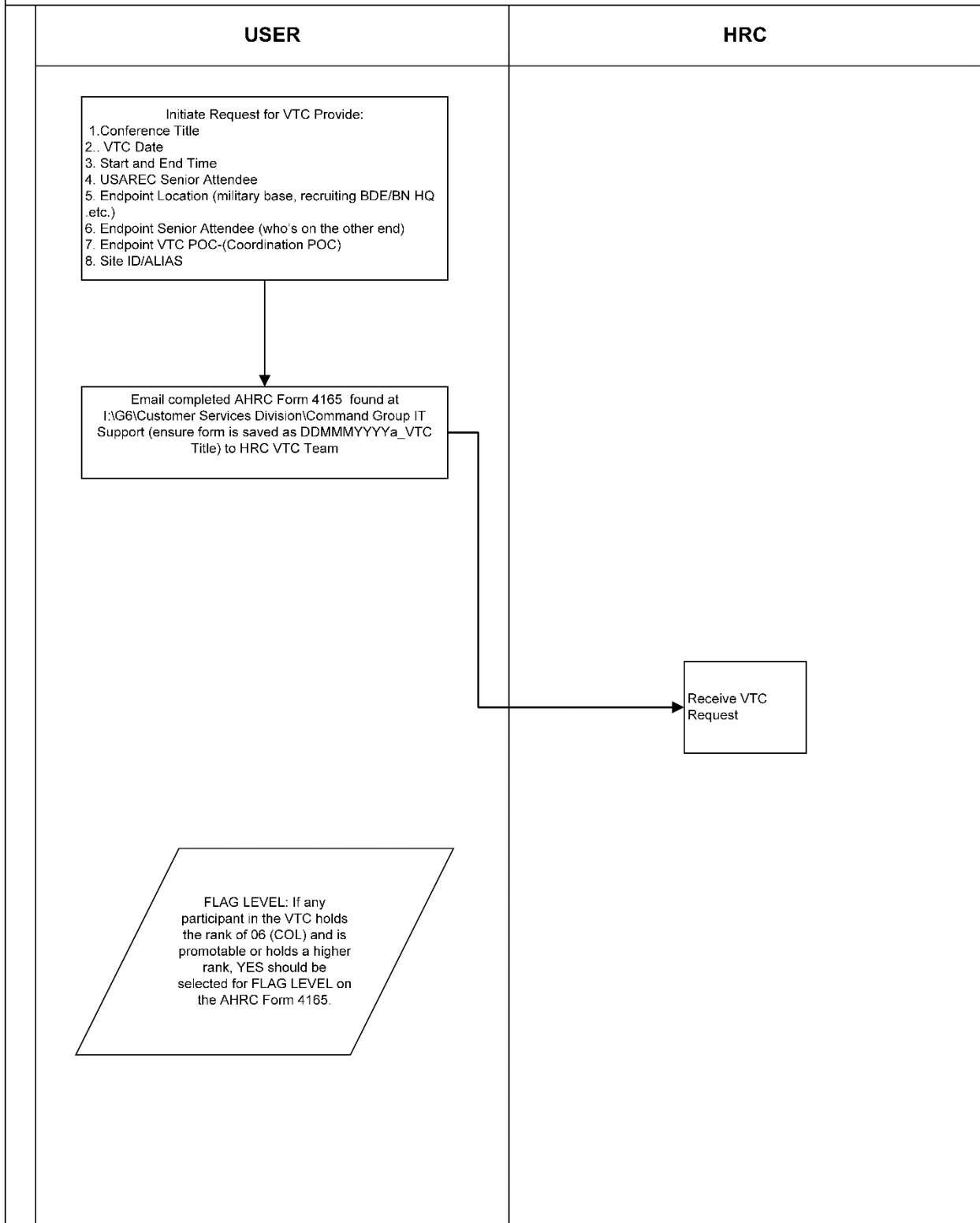


Figure 5-9. Video Teleconference Request Process

Figure 5-10. Software Center Quick Start Guide for Recruiters

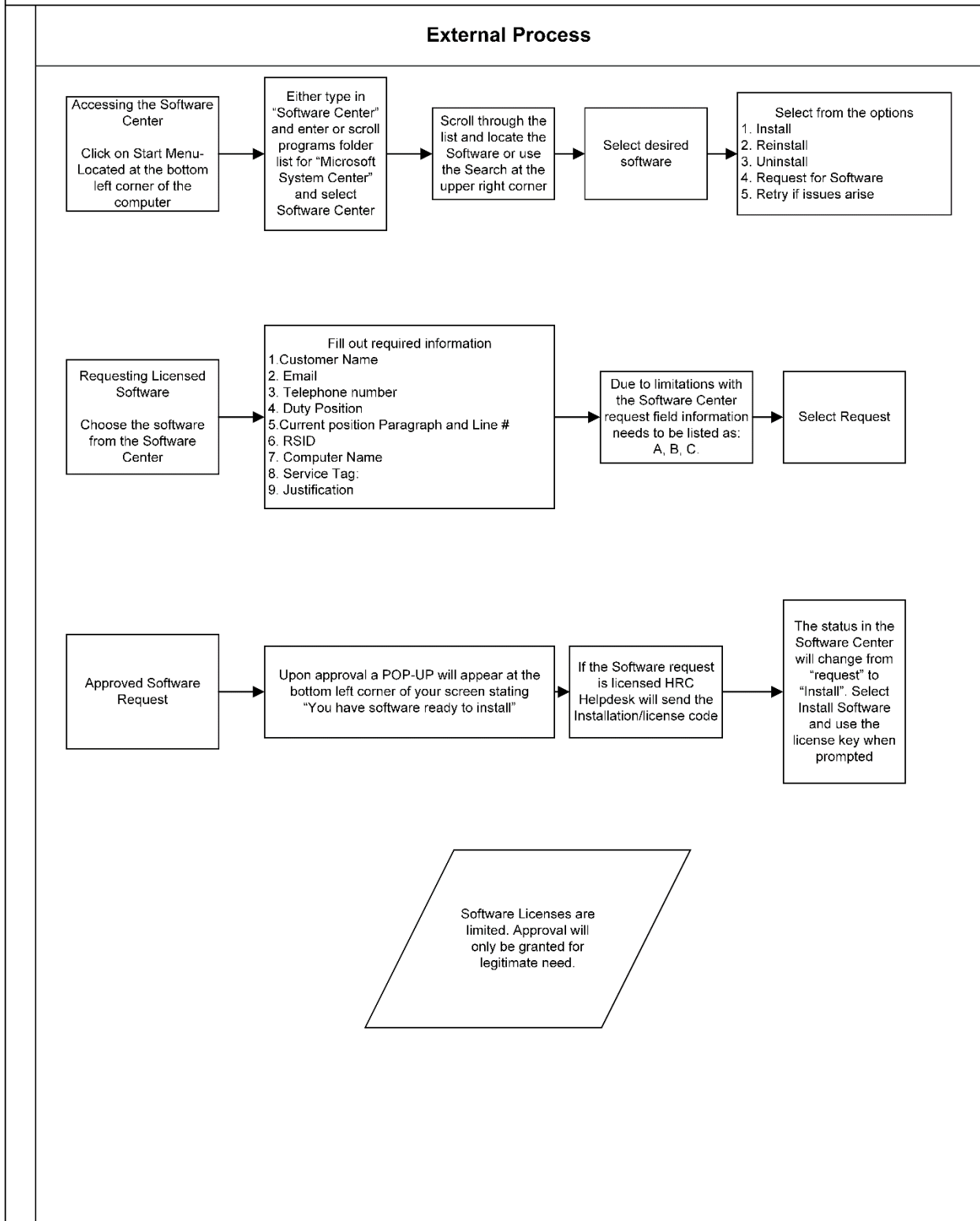


Figure 5-10. Software Center Quick Start Guide for Recruiters

Figure 5-11. HQ IT Support Request Process

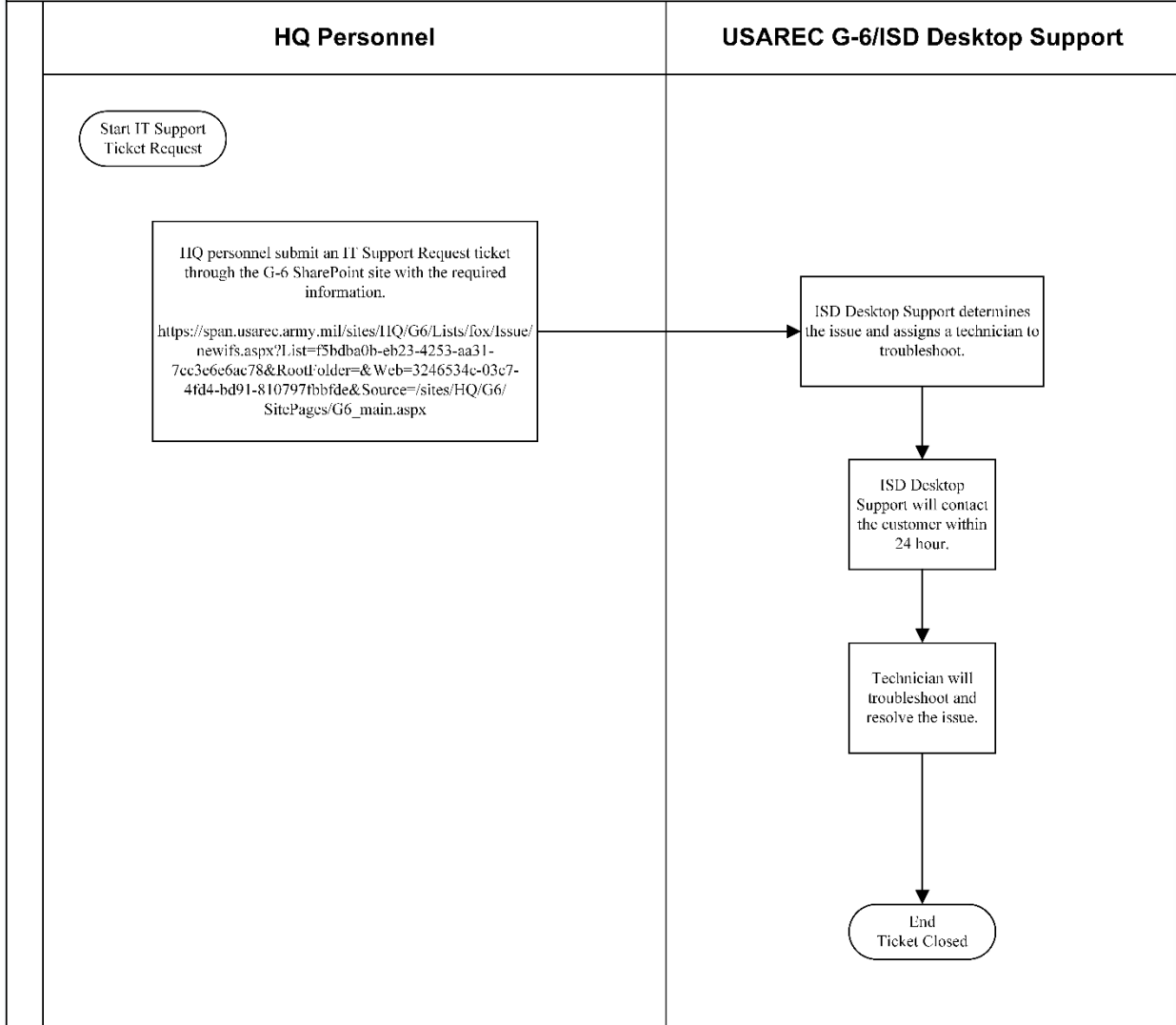


Figure 5-11. HQ IT Support Request Process

Chapter 6.

G-6 Product, Program and Project Management Division (P3MD) Roles and Functions

6-1. Product, Program and Project Management Division (P3MD)

P3MD's roles within USAREC G6 is to 'Bring value to USAREC'; the vision is to Provide and integrate technical solutions supporting USAREC's success. The mission of P3MD is 'Connecting the Force that Provides the Strength' by defining technical requirements for IT products, integrating IT programs and executing technical projects for and across USAREC, enabling the command's overall mission accomplishment.

6-2. P3MD is comprised of three disciplines.

Portfolio Management, Product Management, and Program Management. Portfolio Management Branch has Portfolio Managers and Business Analysts. Product Management consists of both a Products Lead and Project Managers. Finally, Program Management is staffed by a Lead Program Manager and Project Managers. All three disciplines will leverage Business Analysts as necessary within their individual business processes. (See Figure 6-1 for structure)

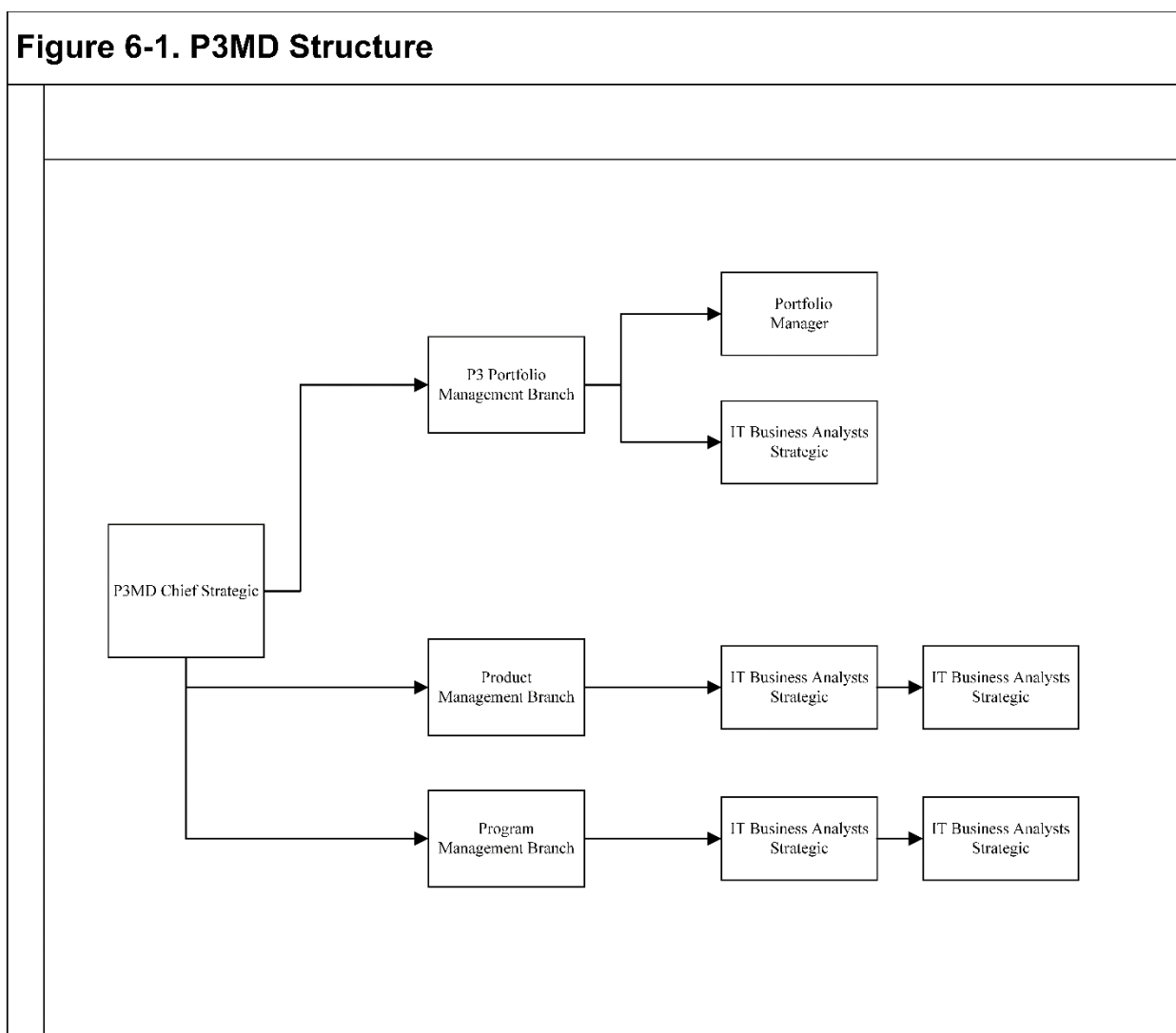


Figure 6-1. P3MD Structure

6-3. List of responsibilities and functions

a. P3 Portfolio Management. Portfolio Management Discipline is concerned with the strategic level of USAREC. Reviewing emergent technologies to enhance recruiting efforts, aligning resources to strategic goals, and assessing risk tolerance using a business analyst discipline. This discipline tracks and aligns priorities, resources and emerging technology to enhance the recruiting mission.

b. Portfolio Manager Functions:

(1) Provide a framework for analyzing, planning and executing technology creating and measuring business value of IT for the USAREC mission.

(2) Create and maintain a portfolio of past, present, and future products and programs to include the projects associated with each.

c. IT Business Analyst functions:

(1) Point of entry for all strategic business or operational service through justified requests in support of USAREC HQ, Brigades, Battalions and Stations to include solutions for IT equipment life cycle replacement (LCR) or emerging technology research.

(2) Focus on the organizational business needs and recommend changes wherever required.

(3) Analyze and assess USAREC's technology requests through the collection of requirement(s) from requestor, including stakeholders, to determine commander's intent, and scope of the request.

(4) Using one-on-one interviews, surveys or facilitated meetings, create user stories to gain an in-depth understanding of specific business needs and/or deliverables.

(5) Develop business relationships with USAREC staff elements to ensure a full understanding of the problem is defined.

(6) Based on documented collected requirements; collaborate with other USAREC HQ G6 branches to forecast cost and deliverable dates.

(7) Gain approval of documented requests.

d. P3 Product Management overview:

(1) Product management is an organizational lifecycle function dealing with the planning, forecasting, and production, or distribution of a product or products at all stages of the product lifecycle.

(2) Product Management is also concerned with strategic alignment through:

- Gathering the "Voice of the User(s)" (problems to be solved – Demand Management)
- Identifying new products (defining requirements and sustainable value)
- Executing the Command's Vision (Command's Roadmap)
- Product success measurements
- Changing Landscape (reinvent or affect change)

e. Product Management functions:

(1) Attending USAREC strategic meetings to determine if a new technology will enhance the recruiting mission.

(2) Ensuring P3MD is a stakeholder in command technical decisions and planning.

(3) Develop business relationships with USAREC staff elements to ensure a full understanding of the business needs and desired outcomes.

(4) After approval of documented products request (function of BA above) create a roadmap and strategy to introduce the product to USAREC including training and support.

(5) Establish guidelines for sunseting or replacement of the product once it is no longer of business value to USAREC's mission.

f. P3 Program Management overview.

(1) Program management is the process of managing several related projects, with the intention of improving an organization's performance. Program management is closely related to change management, and business transformation.

(2) Program Management Branch is concerned with the tactical activities of USAREC such as connecting strategic planning with implementation. Collaborating and coordinating shared goals with the Service Provider, USAREC directorates and the G6 divisions. Furthermore, ensuring program goals are met through oversight of projects and changes for and within programs, identifying the purposes and statuses and continuous improvement to the program.

g. Program Management functions:

- (1) Develop detailed plans, goals, and objectives for long and short range planning, programming, implementation and administration of organizational and programmatic goals.
- (2) Provide a decision-making capacity that cannot be achieved at project level or by providing the project manager with a program perspective when required, or as a sounding board for ideas and approaches to solving project issues that have program impacts.
- (3) Determine the impact of any program changes requested from within USAREC and gain approval for change once clarified and a full understanding is received from all stakeholders.
- (4) Prioritize across the organization and with service provider through collaboration and coordination to aid in successful delivery of individual projects for programs to ensure USAREC attains mission benefits needed when required.
- (5) Ensure program changes are completed in a timely manner (based on the Recruiting Calendar) without disruption to USAREC, especially to the individual recruiter.
- (6) Track service and/or change request relating to program context, including the overall changes made by service provider to ensure USAREC strategic goals are met and benefits are received.

h. Project Managers.

(1) Project managers coordinate a set of tasks at an operational level as project management is the practice of the work of a team to achieve specific goals and meet specific success criteria at the specified time. A project is a temporary endeavor undertaken to create a unique product, service or result. The primary challenge of project managers is to achieve all of the project goals within the given constraints.

(2) Project Management functions:

- (a) Using the approved cost, schedule and scope documentation from the Business Analysts, determine which project management framework suits the project.
- (b) Gain approval of resources needed to complete project.
- (c) Create a project plan with milestones or sprints, based on framework.
- (d) Establish a stakeholder register and communications plan to manage project expectations.
- (e) Initiate risk management.
- (f) Manage changes to the project.
- (g) Resource Management, to include budget management, early user testing, and support.
- (h) Ensure training for new product or program change is written concisely with easy to understand language.
- (i) Transition into operations or sunset product or program.
- (j) At project completion, to the satisfaction of the requestor, create project closure documents and/or after action reports (AAR(s)).

i. The following functions are the responsibility within P3MD:

- (1) Create OPORD or TASKORDs, as needed, to gain support for USAREC approved product(s) or program(s), or projects.
- (2) Coordinate any product, program or project support required with service provider, as needed.
- (3) Discuss specific requirements, due outs or deliverables with stakeholders through meetings or working groups facilitated either through USAREC or service provider.
- (4) Budgetary requirements. In addition to determining whether a Memorandum of Understanding (MOU) or Service Level Agreement (SLA) is required
- (5) Continuous improvement.
- (6) Lifecycle planning.
- (7) Create measurements (metrics).

j. Project Management division business processes.

- (1) Products, Programs and Project Management Division (P3MD) Process Overview (see Figure 6-2).
- (2) Input of Change into HRC Business Process Request (BPQ) Process (see Figure 6-3).
- (3) End User Testing (EUT) for Major HRC Software Changes. (See Figure 6-4).
- (4) Laptop Lifecycle Replacement (LRC) Today (see Figure 6-5).

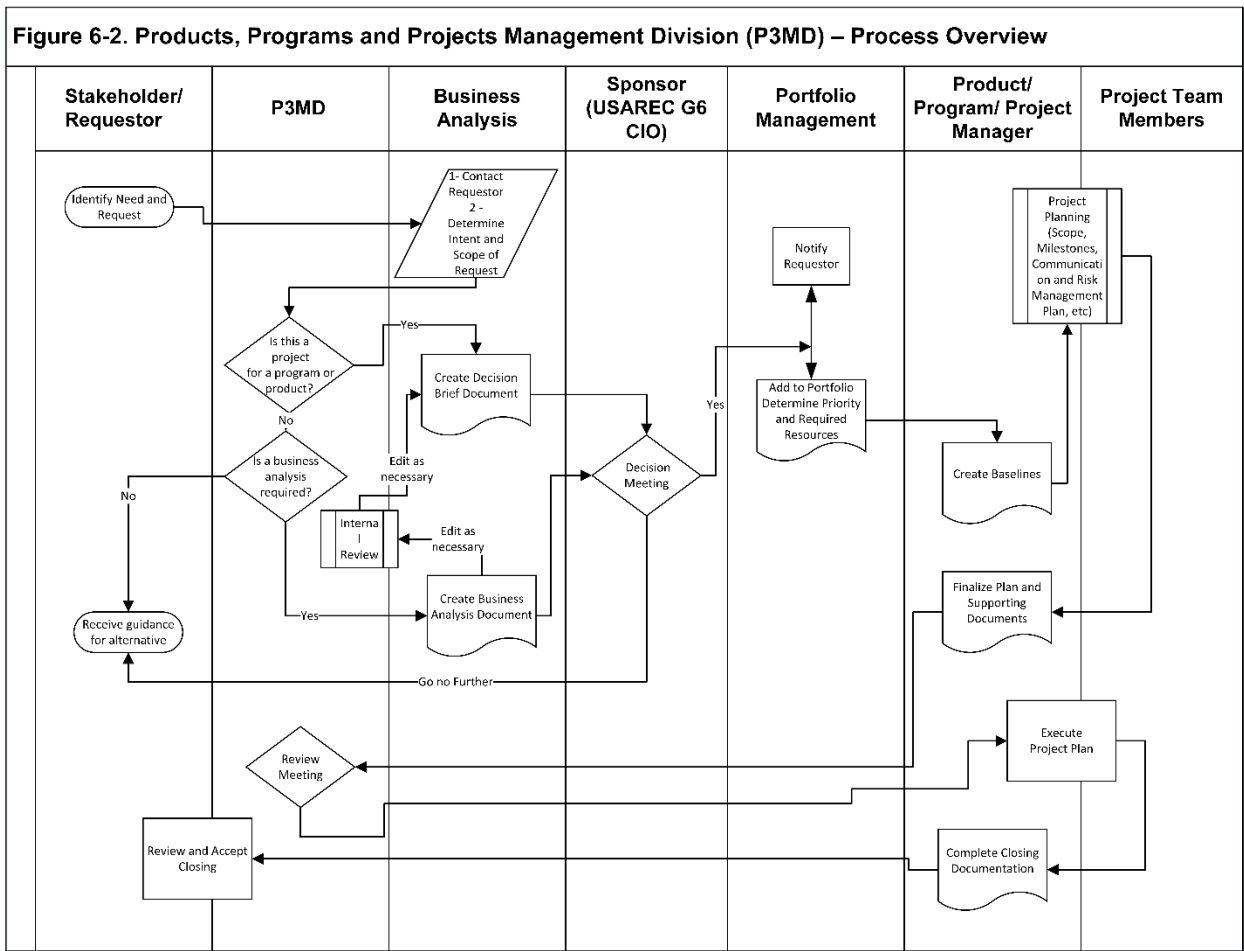


Figure 6-2. Products, Programs and Project Management Division (P3MD)-Process Overview

Figure 6-3. Input of Change into HRC Business Process Request (BPQ) Process

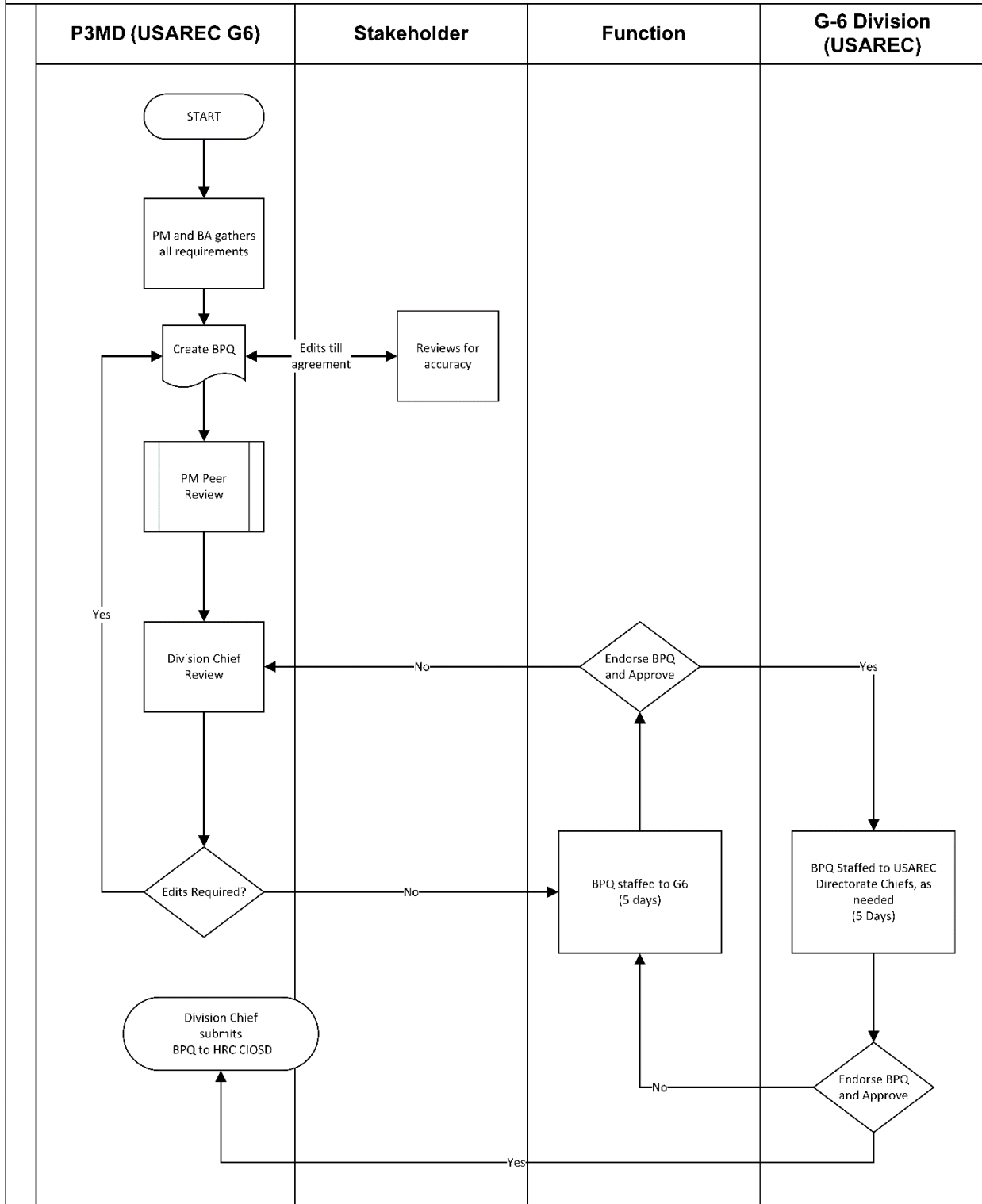


Figure 6-3. Input of Change into HRC Business Process Request (BQP) Process

Figure 6-4. End User Testing (EUT) for Major HRC Software Changes Pg.1

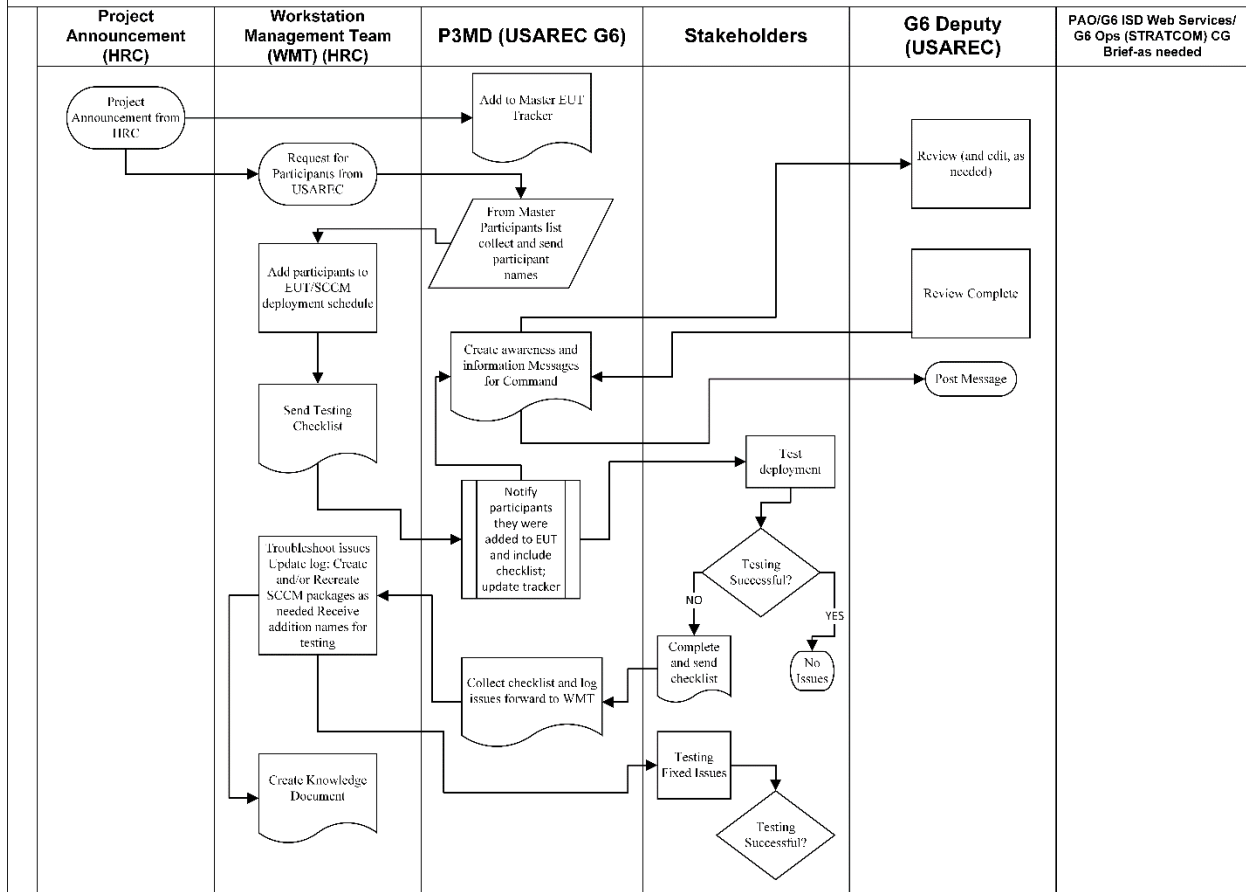


Figure 6-4. End User Testing (EUT) for Major HRC Software Changes Page 1

Figure 6-4. End User Testing (EUT) for Major HRC Software Changes Pg.2

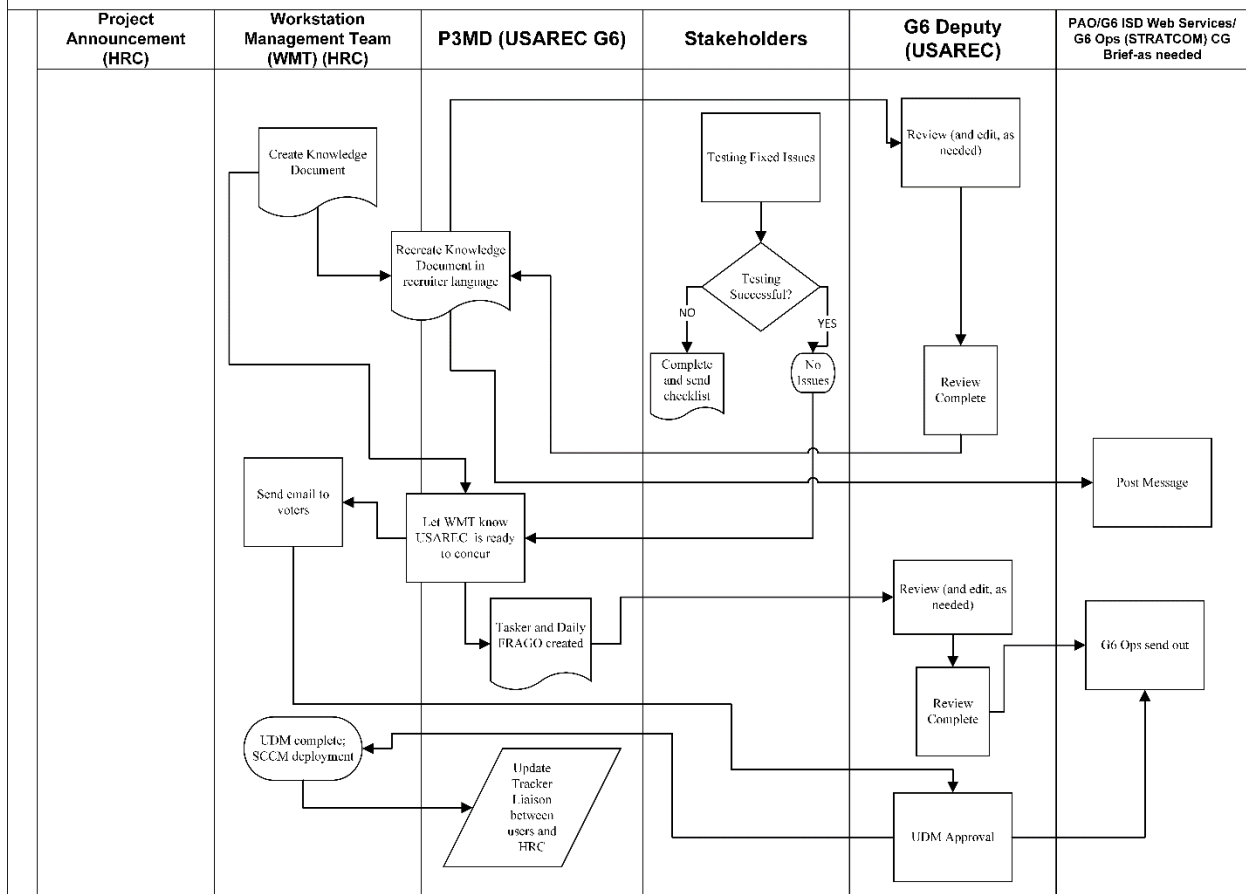


Figure 6-5. End User Testing (EUT) for Major HRC Software Changes Page 2

Figure 6-5. Laptop Lifecycle Replacement (LCR) Today

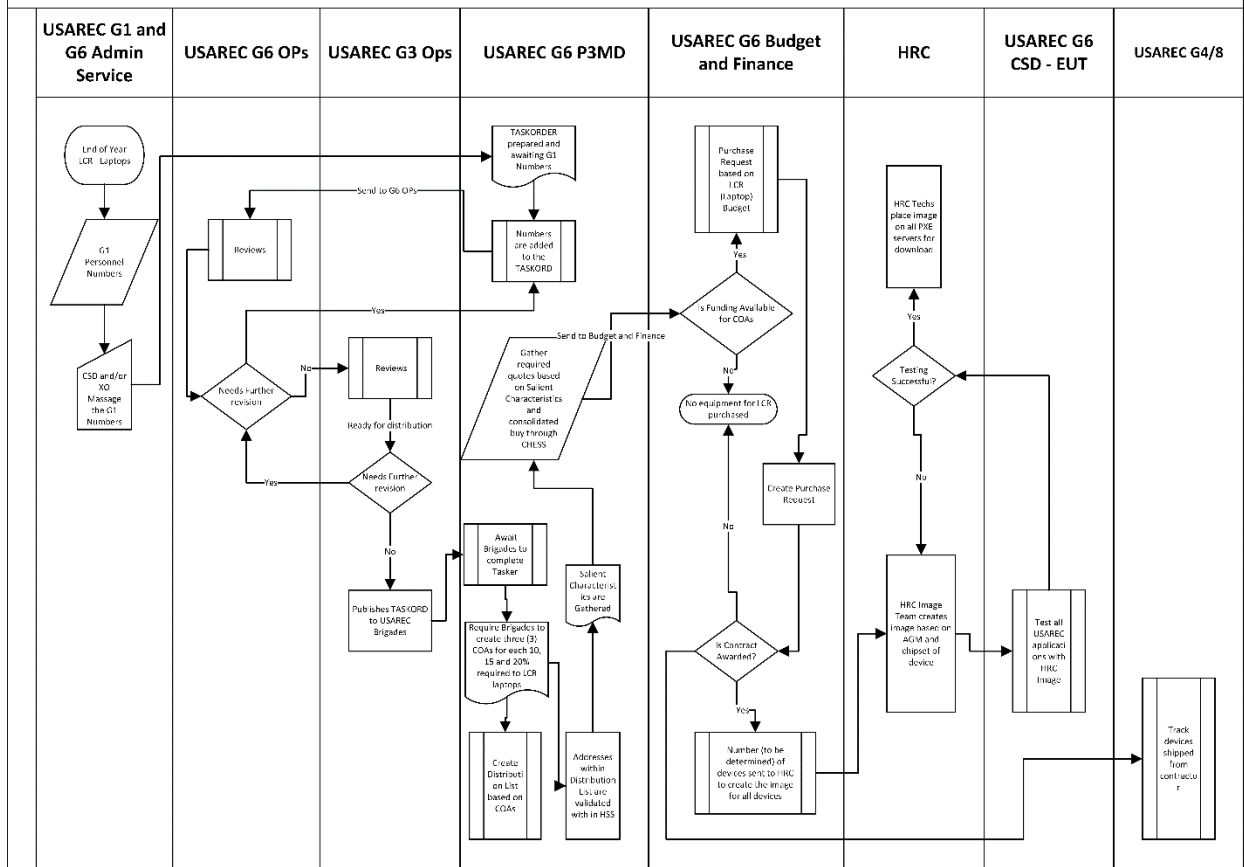


Figure 6-6. Laptop Lifecycle Replacement (LCR) Today

Chapter 7.

S-6 Brigade/Battalion Level Roles and Responsibilities.

7-1. IT Specialists

IT Specialists assigned to the BDE and BN level organizations serve as the principal staff officers for the S-6 section within their organizations. The S-6 ensures the commander can communicate to facilitate effective mission command of their respective units.

7-2. S-6

The S-6 is responsible for the voice/data communications assets within their organization. They report to the Executive Officer, and interact with the S-3 and other staff officers to determine specific or unique communications and network requirements.

a. The S-6 provides customer service, technical assistance, and support to their respective organizations on a variety of IT equipment, software products and non-procedural computer languages and telecommunications on Army Information Systems (AIS) and the DOD Information Network (DODIN). This includes network management and operations, continuity of operations, disaster recovery operations, and workstation management. Also responsible for the administration and adherence of systems and users in their organizations with regulatory guidance, formal publications and USAREC command policies.

b. Responsibilities also include presentation of their commander's IT priorities and issues to the G-6 for awareness, consideration, adjudication, and staff coordination.

c. IT support normally begins with the end user via self-help products and aids, or other venues as noted below:

(1) Matters and issues with ARISS applications and services on the RSN will be addressed via our Service Provider's Help Desk at telephone (502) 613-7777, or toll-free 877-272-1330, or email mailto:usarmy.knox.hrc.mbx.it-help-desk@mail.mil.

(2) IT hardware issues should be addressed to the appropriate S-6 section. This includes matters pertaining to desktop, laptop and tablet computing devices, and voice/data communications hardware.

(3) Many issues (telecommunications, cyber/IA, Requests for Information, web service support requests, project proposals, etc.), can be addressed via the HQ USAREC G-6 IT Support Requests web-site at <http://span.usarec.army.mil/sites/HQ/G-6/SitePages/G-6%20Requests.aspx>

(4) Mobile device hardware issues should be addressed by their respective S-6, but [can also be addressed by HQ USAREC](#) with creation of a ticket on the USAREC IT Support Requests web-site at: <http://span.usarec.army.mil/sites/HQ/G-6/SitePages/G-6%20Requests.aspx>

(5) [Other support issues should be directed to the HQ USAREC G-6 Desktop Support Branch](#) at mail to: usarmy.knox.usarec.mbx.hq-G-6-desktop-support-team@mail.mil

(6) Additional information and assistance is also available by addressing them directly to the appropriate offices listed below:

(7) Cybersecurity/Information Assurance Division: mail to: usarmy.knox.usarec.mbx.hq-G-6-ia-officer@mail.mil

(8) Information Technology Business Office Division for matters related to financial management: mail to: usarmy.knox.usarec.mesg.hq-G-6-governance@mail.mil

(9) Freedom of Information Act/Privacy Act Team: mail to: usarmy.knox.usarec.list.hq-G-6-foia@mail.mil

(10) Integrated Services Division: mail to: usarmy.knox.usarec.list.hq-G-6-customer-svc-div@mail.mil

(11) Desktop Support Team: mail to: usarmy.knox.usarec.mbx.hq-G-6-desktop-support-team@mail.mil

(12) Mobility Branch for matters related to mobile devices and DEE email encryptions: mail to: usarmy.knox.usarec.list.hq-G-6-trusted-agents@mail.mil

(13) Network Operations, including voice communications (land line POTS & VOIP): mail to: usarmy.knox.usarec.list.hq-G-6-netops@mail.mil. Tech Ops: mail to: usarmy.knox.usarec.list.hq-G-6-techops@mail.mil

(14) Network Operations Early User Test: mail to: usarmy.knox.usarec.mbx.hq-G-6-eut@mail.mil

(15) Products, Programs and Project Management Division: mail to: usarmy.knox.usarec.list.hq-G-6-projects@mail.mil

Chapter 8.

G-6 In/Out Processing Procedures

8-1. Purpose.

This chapter standardizes policies and procedures for processing personnel arriving or departing the Headquarters Staff, with the goal of providing an all-inclusive process with an enhanced user experience.

8-2. Army Acculturation Program.

The attached process maps and forms were designed to assist personnel processing in or out of the Headquarters Staff. These policies, processes and procedures can also be integrated into established procedures at lower level organizations.

8-3. Summary, Scope and Assumptions.

Please provide recommendations for improvement to the Prepotency identified on the front page of this publication.

8-4. In-Processing Responsibilities.

Directorate (see Figures 8-1 and 8-2)

8-5. Arrival Requirements.

a. Pre-Arrival

- (1) Provide information on arrivals to the G-6.
- (2) Provide IT equipment to Client Services or Device Management for user prep at least 5 working days prior to user arrival if needed.

b. Post-Arrival.

- (1) Verifies the User has reported into HHC and has "been arrived" in HSS. Issues the UF 25-1-1.1 (User In-Processing Checklist (Directorate Checklist) to the user.
- (2) Once the user completes Part 1, and Supervisor completes Part II of the DD Form 2875, submit the DD Form 2875 to the Security Office to gain access to the RSN.
- (3) Add User to applicable Enterprise Email distribution lists and shared mailboxes.

c. USAREC Security Officer.

- (1) Process DD Form 2875.
- (2) Forward to G-6 CYBER Division.

d. USAREC Contracting Officer (for Contract Personnel).

- (1) Input user into Trusted Associate Sponsorship System (TASS).
- (2) Notify Contractor when to receive Common Access Card (CAC).

e. User Military and DA Civilian).

- (1) Report to HHC for In-Processing checklist; Reference Fig 8-6.
- (2) Army Training & Certification Tracking System (ATCTS) (<https://atc.us.army.mil>).
- (a) Verify completion of required Information Awareness training on ATCTS.
- (b) Change Signal Command/FCIO to:
 - (c) 7th Signal Command (Theater)-Fort Gordon-->93rd Signal Brigade(93d Sig Bde)-->Bluegrass Region-->Installation Fort Knox-->Human Resources Command -Fort Knox(HRC)-->RSN / RSNi (RSN)-->US ARMY RECRUITING COMMAND(USAREC)-->HQ USAREC.

(d) Change AC to:

Training & Doctrine Command (TRADOC) -->US ARMY RECRUITING COMMAND (USAREC) -->HQ USAREC.

- (e) Remove all non-applicable documents (i.e. Privileged Access Agreements and Duty Appointment Orders).
- (f) Cybersecurity Training Center (<https://ia.signal.army.mil/DoDIAA/default.asp>).
 - Login to site and sign updated AUP.
 - MilConnect (<https://www.dmdc.osd.mil/milconnect/>).
 - Update profile contact information for duty location.
 - Register/Update profile information in the Mass Warning & Notification System (MWNS) (<https://>

alert.csd.disa.mil/Self Service DOD).

- Request New User computer setup from Client Services
- Request New User mobility equipment setup from the Mobility Team if user is authorized
- Attend Monthly G-6 Brief.

f. User (Contract Personnel)

(1) Receive CAC from One-Stop once notified by Supervisor/COR

(2) Army Training & Certification Tracking System (ATCTS) (<https://atc.us.army.mil>)

(a) Verify completion of required Information Awareness training on ATCTS.

(b) Change Signal Command/FCIO to:

(c) 7th Signal Command (Theater)-Fort Gordon--93rd Signal Brigade(93d Sig Bde)--Bluegrass Region--Installation Fort Knox--Human Resources Command-Fort Knox (HRC)--RSN/RSNI (RSN)--US ARMY RECRUITING COMMAND (USAREC)--HQ USA REC.

(d) Change AC to:

(e) Training & Doctrine Command (TRADOC) --US ARMY RECRUITING COMMAND (USAREC) --HQ USAREC.

(f) Remove all non-applicable documents (i.e. Privileged Access Agreements and Duty Appointment Orders).

(g) Cybersecurity Training Center (<https://ia.signal.army.mil/DoDIAA/default.asp>). Log into site and sign update AUP.

(h) MilConnect (<https://www.dmdc.osd.mil/DoDIAA/default.asp>). Update profile contact information for duty location.

(i) Register/Update profile information in the Mass Warning & Notification System (MWNS) (<https://alert.csd.disa.mil/Self Service DOD>).

(j) Request New User computer setup from Client Services.

(k) Request New User mobility equipment setup from the Mobility Team if user is authorized.

(l) Attend Monthly G-6 Brief.

g. G-6 Cybersecurity Division.

(1) Verify administrative accuracy and completeness of the DD Form 2875.

(2) Verify user has an active account in HSS.

(3) Verify user has active record in ATCTS.

(4) Verify user's Annual Cyber Awareness training is current.

(5) Verify user's Army Acceptable Use Policy (AUP) is current.

(6) Mover user's ATCTS account to HQ USAREC container.

(7) Activate user record in IMS.

(8) Generate message to HRC IT Help Desk requesting setup of new RSN User Account. Add the Cybersecurity Office, the Desktop Support Team, and user Branch/Division Chiefs to the cc line of the message

(9) Submit for REQUEST account if user is authorized.

(10) Create user Google GoArmy account if user is authorized.

h. G-6 Integrated Solution Division.

(1) Desktop Support Branch Technician will perform New User Computer Setup.

(2) Mobility Branch Technician will perform New User equipment setup if authorized.

8-6. Out-Processing Responsibilities

a. Directorate (see Figures 8-6).

(1) Provide information on departures to the G-6. Issues the user a UF 25-1-1.3 (Directorate Out-processing Checklist). Ensure User is removed from Enterprise Email Distribution Lists and Shared Mailboxes

(2) Hand Receipt holder receives IT equipment and advises G-6 Mobility Team to deactivate mobile devices if user was authorized.

(3) Submit DD2875 to deactivate RSN account if applicable.

b. USAREC Security Officer.

(1) Process DD Form 2875 if applicable.

(2) Forward to G-6 Cyber Division.

c. USAREC Contracting Officer (for Contract Personnel). Collect CAC.

d. User Military and DA Civilian.

(1) Report to HHC to receive Command Out-Processing Checklist.

(2) Request assistance from G-6 Integrated Solution Division if data transfer is needed.

(3) Present mobile devices to the G-6 Mobility Team for deactivation if authorized.

(4) Turn-in IT equipment to Hand Receipt holder.

(5) Notify G-6 Cyber Division of departure status for Google Data transfer if applicable.

e. Use (Contract Personnel).

(1) Request assistance from G-6 Integrated Solutions Division if data transfer is needed.

(2) Present mobile devices to the G-6 Mobility Team for deactivation if authorized.

(3) Turn-in IT equipment to Hand Receipt holder.

(4) Notify G-6 Cyber Division of departure status for Google Data transfer if applicable.

(5) Turn-in CAC to USAREC Contracting Officer.

f. G-6 Cyber Division.

(1) Deactivate ATCTS user account.

(2) Deactivate RSN account in IMS.

(3) Email notification of user account inactivation to SharePoint Team for removal of SharePoint permissions, if applicable.

(4) Request account is locked or deleted.

(5) Google GoArmy account is transferred or deleted.

g. G-6 Integrated Solution Division.

(1) Client Services Technician will transfer data if requested.

(2) Client Services Technician will verify user has been removed from Enterprise Email Distribution Lists and Shared Mailboxes.

(3) Mobility Technician will wipe and deactivate mobile devices if user was authorized.

(4) Mobility Technician will deactivate MobileIron account.

8-7. Maintenance

a. G-6 will be responsible for ensuring timely review and revision of procedures, briefing pamphlets, user and directorate checklists and HHC process submission updates.

b. G-6 Divisions will be responsible for the review and revision of internal processes semiannually.

c. USAREC Form 25-1-1.1 "G-6 User In-Processing Checklist" will be used by all users in-processing USAREC Headquarters with an IT requirement.

d. Cyber division business processes.

(1) G-6 In-Processing (Military and DA Civilian) (see figure 8-1)

(2) G-6 In-Processing (Contract Personnel) (see figure 8-2)

(3) G-6 Out-Processing (Military and DA Civilian) (see figure 8-3)

(4) G-6 Out-Processing (Contract Personnel) (see figure 8-4)

(5) G-6 User In-Processing Checklist UF 25-1-1.1 (figure 8-5)

(6) G-6 Directorate In-Processing Checklist UF 25-1-1.2 (see figure 8-6)

(7) G-6 Directorate Out-Processing Checklist UF 25-1-1.3 (see figure 8-7)

(8) G-6 User Out-Processing Checklist (Military/DA Civilian) UF 25-1-1.4 (see figure 8-8)

(9) G-6 User Out-Processing Checklist (Contract Personnel) UF 25-1-1.5 (see figure 8-9)

Figure 8-1 G-6 In-Processing (Military and DA Civilian)

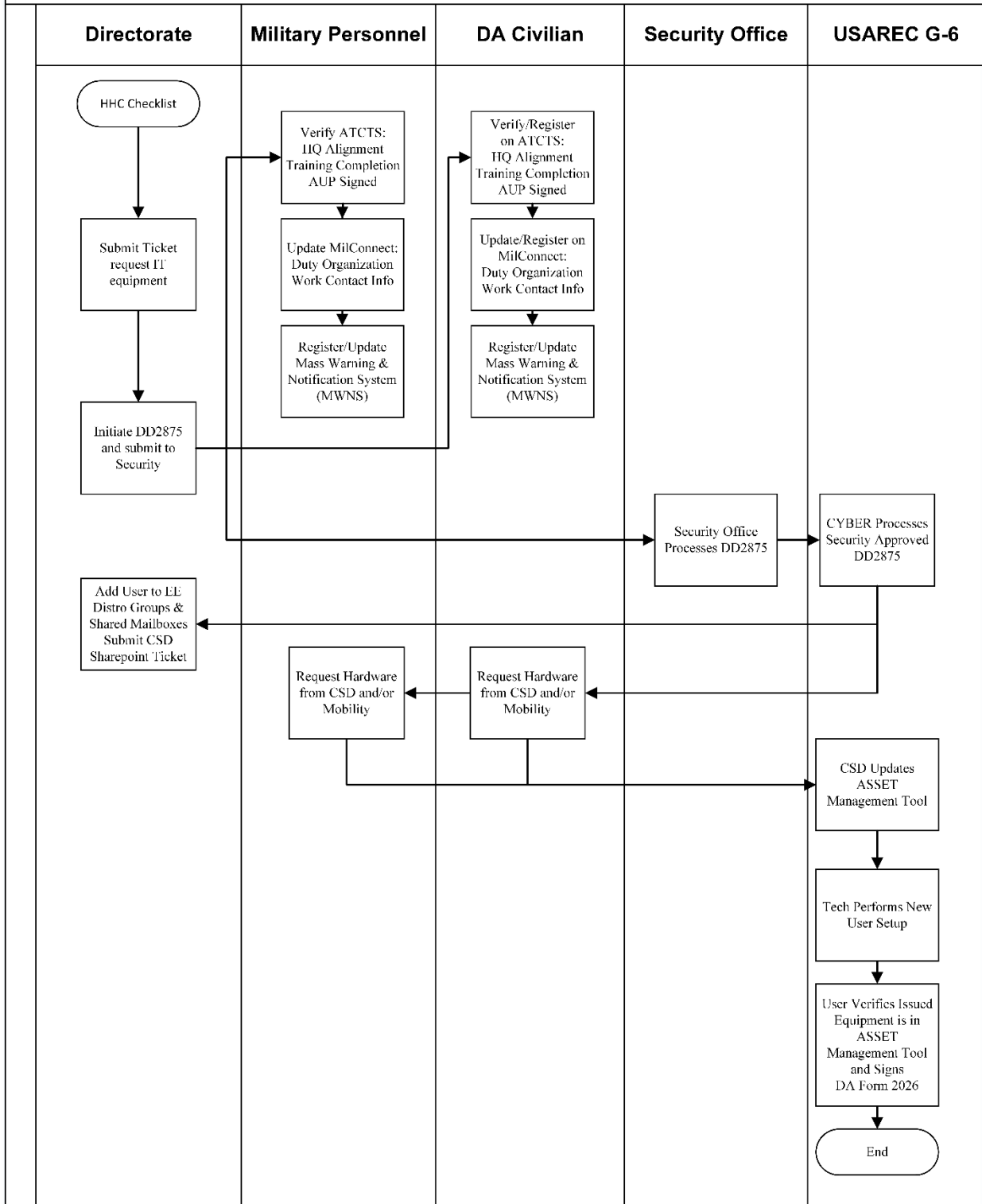


Figure 8-1. G-6 In-Processing (Military and DA Civilian)

Figure 8-2 G-6 In-Processing (Contract Personnel)

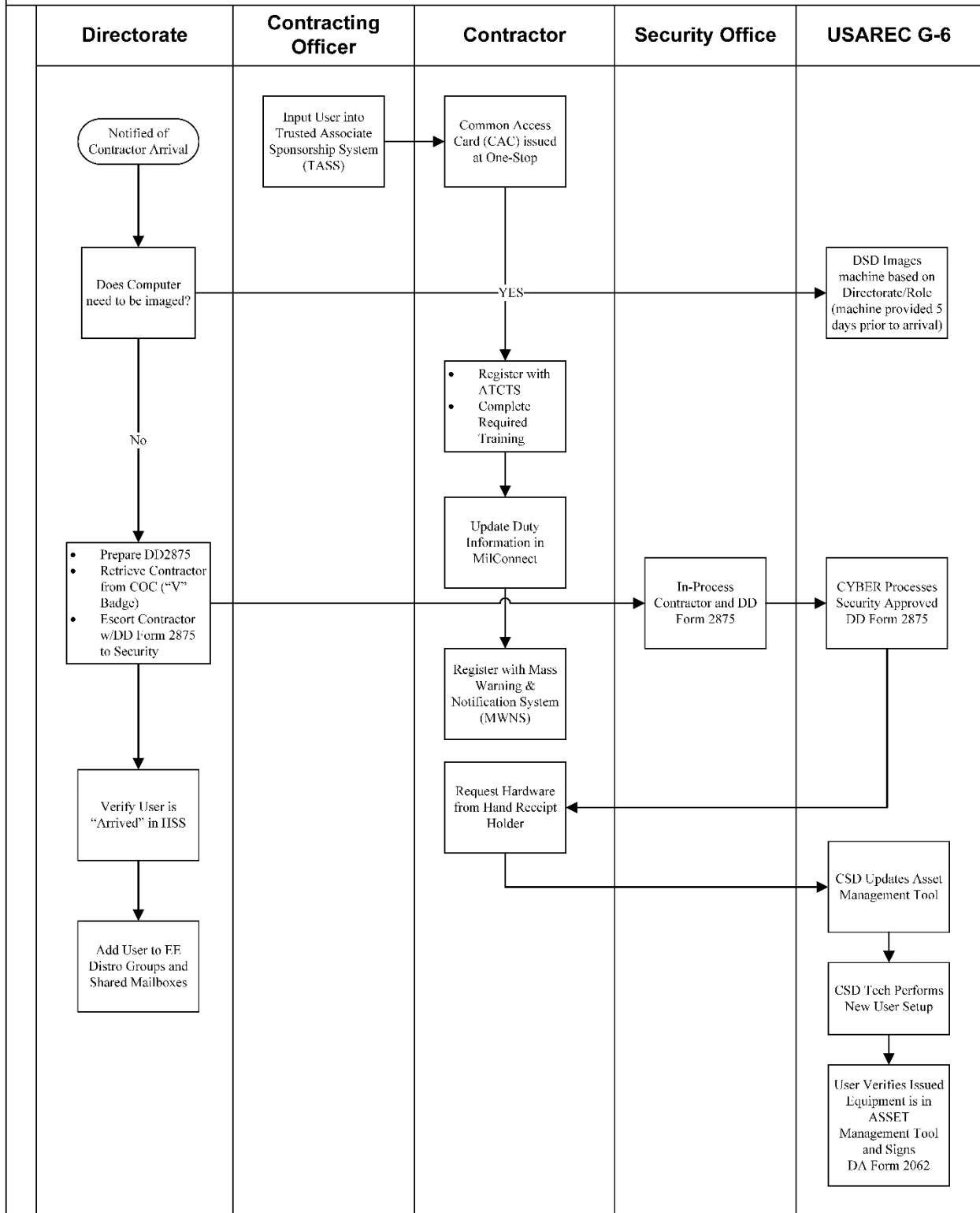


Figure 8-2. G-6 In-Processing (Contract Personnel)

Figure 8-3. G-6 Out-Processing (Military and DA Civilian)

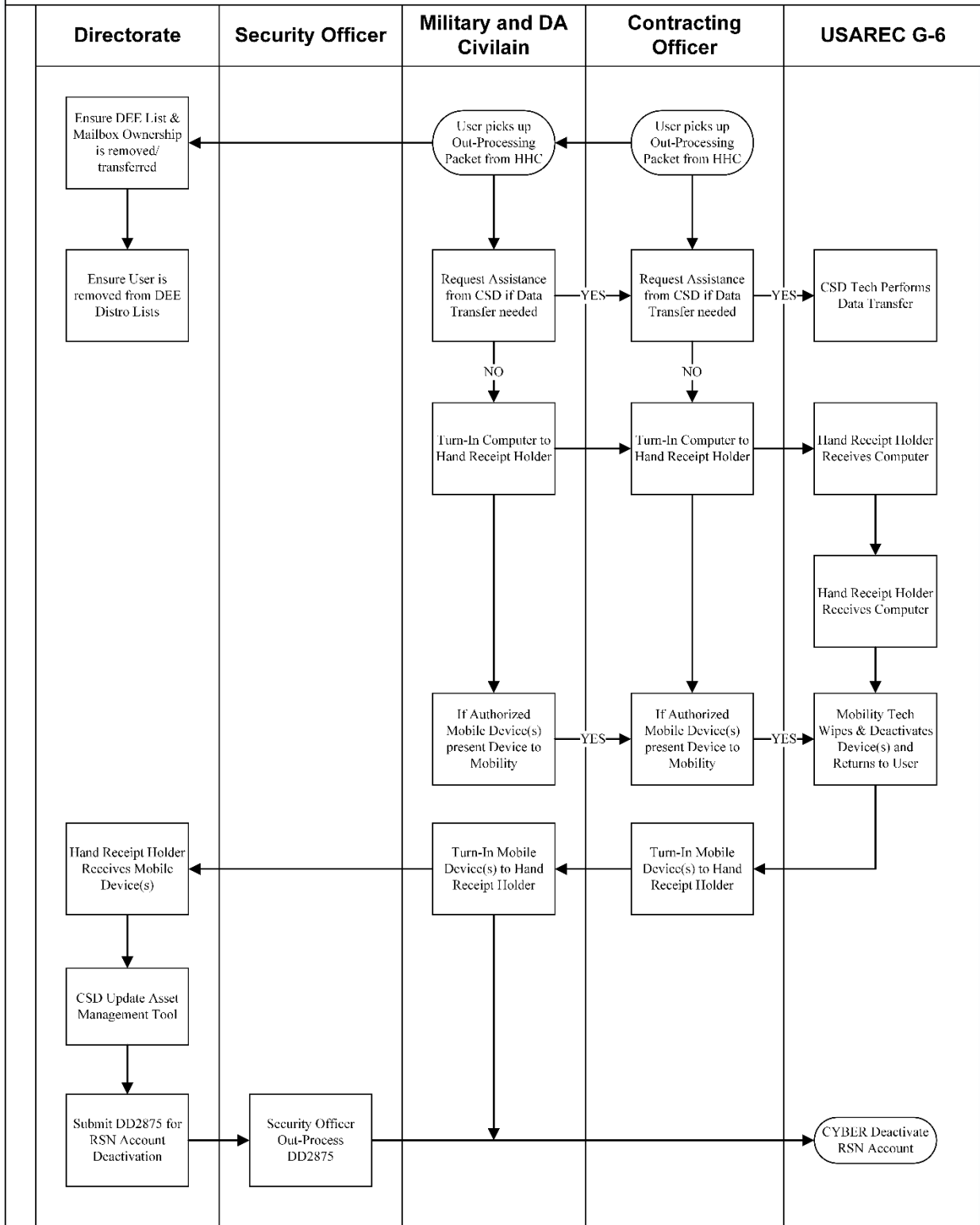


Figure 8-3. G-6 Out-Processing (Military and DA Civilian)

Figure 8-4. G-6 Out-Processing (Contract Personnel)

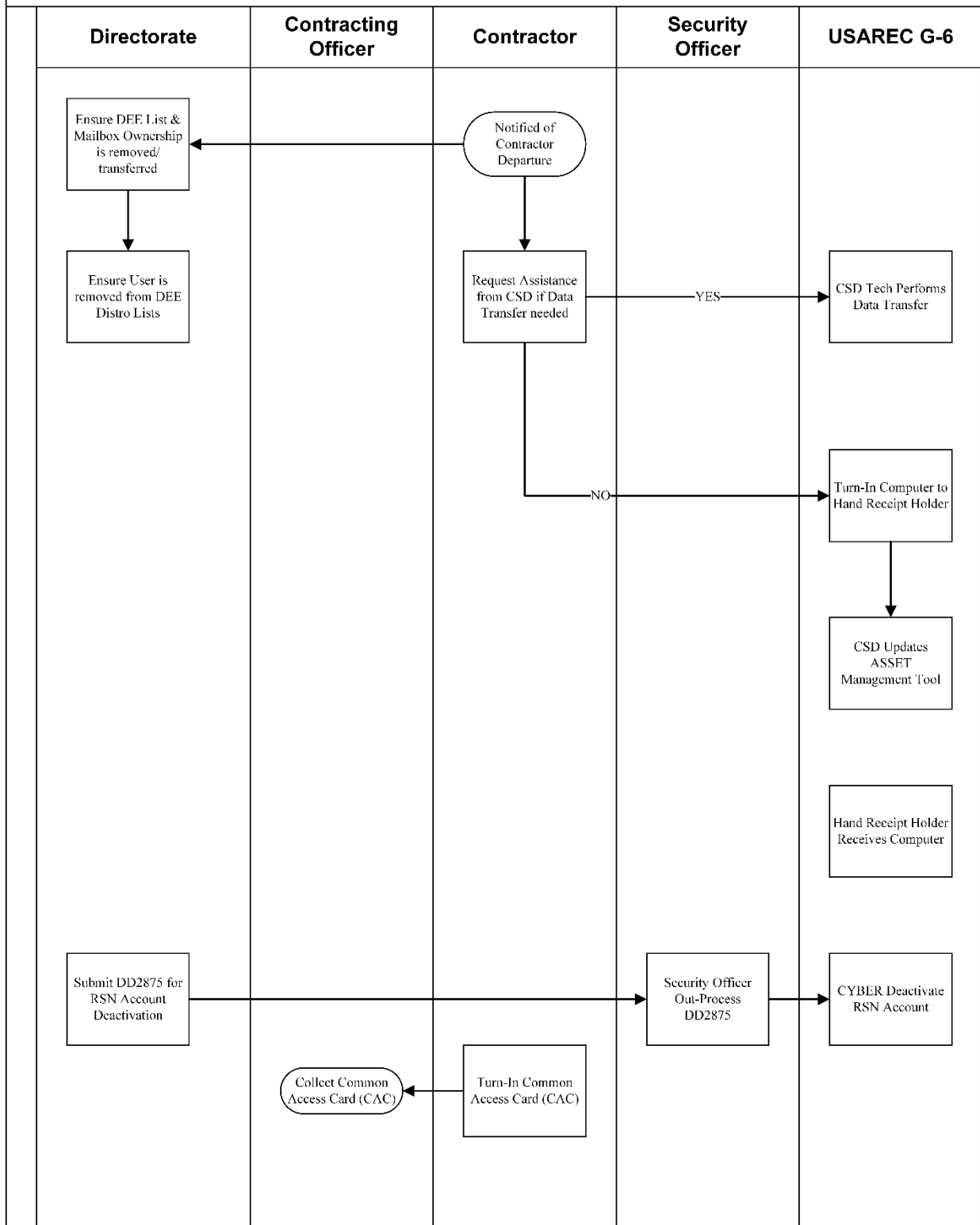


Figure 8-4. G-6 Out-Processing (Contract Personnel)

G-6 User In-Processing Checklist
(For use of this form see USAREC Pam 25-1-1)

		YES	NO	NA
Name	Rank			
Duty Section	Duty Title			
Arrival Date	Departure Date			
<p>To ensure your enterprise account experience remains running smoothly:</p> <p>a. Army Training and Certification Tracking System (ATCTS) (USER).</p> <p>1). Open https://atc.us.army.mil/iastar in Internet Explorer and log in.</p> <p>2). Click "Edit Account Info".</p> <ul style="list-style-type: none"> • Verify Enterprise Email address is accurate and up to date. <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> NA • Verify Desk Phone number is accurate and up to date. <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> NA • Change HQ Alignment Unit to USAREC. <ul style="list-style-type: none"> o Click "Search for Unit" o Type USAREC in the Unit Search box and click OK. o Click "open" next to USAREC o Choose the location you are assigned to (click "Select" next to USAREC). o You will be prompted to use USAREC for the Signal Command/FCIO unit as well. Choose Yes. o Click "Update" at the bottom of the page. <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> NA <p>3). Verify dates of the following training, if any training is missing or expired, you must complete training or your account will be suspended.</p> <ul style="list-style-type: none"> • DoD Cyber Awareness Challenge Training; annual training - must be within 1 year of current date. If it has not been taken, is expired or expiring within 7 days, go to the Signal Center Information Assurance Training website: (https://ia.signal.army.mil/DoDIAA/default.asp). <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> NA • WNSF – If you have not taken WNSF training, go to the Information Assurance Virtual Training website (https://iatraining.us.army.mil/). <ul style="list-style-type: none"> o Phishing Awareness v2.0, training only taken once o Portable Electronic Devices and Removable Storage Media v2.0, training only taken once. o Safe Home Computing, training only taken once. o Personally Identifiable Information (PII) v2.0, training only taken once. <p>4). Remove outdated agreements and upload current Acceptable Use Policy (AUP).</p> <ul style="list-style-type: none"> • Scroll to the bottom of the page to the Documents section. Remove any agreements which are no longer applicable, (i.e. Privileged Access Agreement and Duty Appointment Orders) by clicking the red 'X'. <input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> NA • Remove any previous AUP by clicking the red 'X'. • Put the date of AUP's digital signature in the Date Signed box and click send files. <p>5). ATCTS can now be closed.</p>				

Figure 8-5 . G-6 In-Processing Checklist UF 25-1-1.1


	YES	NO	NA
<p>b. MilConnect (To update Global Address List (GAL) information.) (USER)</p> <ul style="list-style-type: none"> • Open https://www.dmdc.osd.mil/milconnect in Internet Explorer. • Click the "Sign In:" button at the upper right.  <ul style="list-style-type: none"> • Click OK on the consent to monitor banner page. • Choose Login under the CAC and have the user choose certificate. (Do NOT select the email Certificate). • In the top right corner of the page check "You are signed in as a ...". Make sure this says Sponsor. • In "I want to..." section, select "Update work contact info (GAL)". <ul style="list-style-type: none"> o In "Personal Status" section: <ul style="list-style-type: none"> *In "Duty Organization", select "United States Army" *In "Duty Suborganization", "select- TRADOC United States Army Recruiting Command". *Enter Office Symbol and "Job Title" information. *In "Duty Installation/Location", select "Fort Knox, KY (incl. Godman AAF)". • In "Address" section: <ul style="list-style-type: none"> o Enter "Address Line 1 ", "City", "State", "Zip", and "Country" fields. • In "Personnel Email Addresses: <ul style="list-style-type: none"> o Select either "Yes" or "No" indicating your notification preference. • Enter any relevant information in the "SIPRNet Email Address", JWICS Email Address: and Phone/ Fax Numbers" sections. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c. Register/Update Mass Warning and Notification System (MWNS) information (https://alert.csd.disa.mil)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e. Ensure you are added to any applicable group mailbox's and distribution lists.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
f. Schedule/Attend the G6 CIO/Monthly Briefing. [REDACTED]			
<input type="checkbox"/> I have received all IT equipment and processed through the required G-6 divisions.			
Signature			
Supervisor/ Sponsor Signature			

Figure 8-6. (Cont.) G-6 User In-Processing Checklist UF 25-1-1.1

G6 Directorate In-Processing Checklist (For use of this form see USAREC Pam 25-1-1)				
Name	Rank	YES	NO	NA
Duty Section	Duty Title			
Arrival Date	Departure Date			
<p>Pre Arrival (Directorate and G6 CSD)</p> <p>1. At least five days prior to arrival, Directorate submits IT Request ticket for device (Desktop or Laptop) that needs imaging and provides device to G6 CSD. ***G6 will NOT accept "mirror another account" under additional software request.***</p> <p>2. G6 CSD images device based on assigned Directorate.</p> <p>3. Directorate requests desktop telephone by using the "USAREC G6 Telecom Request" on the G6 Sharepoint page/IT Support/IT Request Center. If a VOIP account is needed, it must be setup AFTER a user's RSN account is fully up and running. With very few exceptions within the USAREC HQ's, unless a user is assigned to either the Recruiting Operations Center (ROC) or the Cyber Security office, a VOIP account will not be granted, regardless of phone type. Contact the G6 CSD for any questions regarding VOIP accounts.</p> <p>Post Arrival (Directorate and User)*</p> <p>1. Directorate initiates DD2875 -System Authorization Access Request (SAAR) Part I, items 1-12 and forward to user's Supervisor.</p> <p>2. User's Supervisor completes DD 2875 items 13-20b and 27 (optional) and submits to Security Office.</p> <p>3. Directorate adds user to any applicable Directorate mailbox(es) and Distribution List(s), or submit Sharepoint CSD Ticket to request new user mailbox association.</p>				
Signature				
Supervisor/ Sponsor Signature				

Figure 8-7. G-6 In-Processing Checklist UF 25-1-1.2

Figure 8-7. G-6 Directorate Out-Processing Checklist UF 25-1-1.3

G6 Directorate Out-Processing Checklist (For use of this form see USAREC Pam 25-1-1)		YES	NO	NA
Name	Rank			
Duty Section	Duty Title			
Arrival Date	Departure Date			
<ol style="list-style-type: none"> 1. Provide information of departures to the G6. 2. Ensure User is removed from Enterprise Email Distribution Lists and Shared Mailboxes. 3. Hand Receipt holder receives IT equipment and advises G6 Mobility Team to deactivate mobile devices if user was authorized. 4. Submit DD2875 to deactivate RSN account if applicable. 		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Signature				
Supervisor/ Sponsor Signature				

USAREC Form 25-1-1.3, 5 June 2017

(This is a New Form)

V1.00

Figure 8-8. G-6 Directorate Out-Processing Checklist UF 25-1-1.3

G6 User Out-Processing Checklist (Military and DA Civilian)				
(For use of this form see USAREC Pam 25-1-1)				
Name	Rank	YES	NO	NA
Duty Section	Duty Title			
Arrival Date	Departure Date			
1. Request assistance from G6 Customer Service Division if data transfer is needed.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Turn-in IT equipment to Hand Receipt holder.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Hand Receipt holder receives IT equipment and advises G6 Mobility Team to deactivate mobile devices if user was authorized.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Signature				
Supervisor/ Sponsor Signature				

USAREC Form 25-1-1.4, 5 June 2017

(This is a New Form)

V2.00

Figure 8-9. G-6 User Out-Processing Checklist (Military/DA Civilian) UF 25-1-1.4

G6 User Out-Processing Checklist (Contract Personnel)				
(For use of this form see USAREC Pam 25-1-1)				
Name	Rank	YES	NO	NA
Duty Section	Duty Title			
Arrival Date	Departure Date			
<p>1. Request assistance from G6 Customer Service Division if data transfer is needed.</p> <p>2. Turn-in IT equipment to Hand Receipt holder.</p> <p>3. Hand Receipt holder receives IT equipment and advises G6 Mobility Team to deactivate mobile devices if user was authorized.</p> <p>4. Turn-in CAC to USAREC Contracting Officer.</p>		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Signature				
Supervisor/ Sponsor Signature				

USAREC Form 25-1-1.5, 5 June 2017

(This is a New Form)

V2.00

Figure 8-10. G-6 User Out-Processing Checklist (Contract Personnel) UF 25-1-1.5

References

Section I Required Publications

AR 25-1

Army Information Technology.

AR 25-2

Information Assurance.

AR 70-1

Army Acquisition Policy.

DA PAM 25-1-1

Army Information Technology Implementation Instructions.

Section II Related Publications

UR 25-2

USAREC Cybersecurity

AR 25-30

The Army Publishing Program

DA PAM 25-40

Army Publishing Program Procedures

UR 25-30

USAREC Business Cards.

Section III Prescribed Forms

USAREC Form 25-1-1.1

G-6 In/Out Processing Checklist.

USAREC Form 25-1-1.2

G-6 Directorate In-Processing Checklist.

USAREC Form 25-1-1.3

G-6 Directorate Out-Processing Checklist.

USAREC Form 25-1-1.4

G-6 User Out-Processing Checklist (Military/DA Civilian).

USAREC Form 25-1-1.5

G-6 User Out-Processing Checklist (Contracted Personnel).

Section IV Referenced Forms

There are no entries for this section.

Appendix A Procedures for Removal of SSD Card from Dell Venue Tablets and Tablet Turn in.

Section 1. Introduction

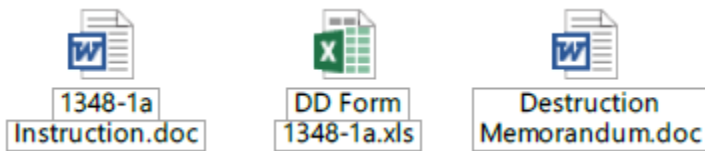
A-1. Purpose

This guide provides the standard administrative procedures for removing SSD card from Dell Venue Tablet Model Number T07G and turn-in procedures for DRMO.

A-2. References

http://www.dla.mil/Portals/104/Documents/DispositionServices/DEMIL/DISP_CPUTurnInGuide_150819.pdf

<https://www.simplix.com/info/ui.shtml>



Section 2. Instructions

A-3. Removing the SSD Card from Dell Venue Tablet.

- a. Take the Dell Venue tablet back plate off.



-
- b. Remove the black film tape that covers the CAC card reader and exposes a green chip with 3 screws.



c. Remove the 3 screws from the green chip.



d. Pull the green chip back to expose the SSD card location



e. Take a pair of needle nose pliers and remove the SSD card.



f. After the SSD card has been removed it will look like this

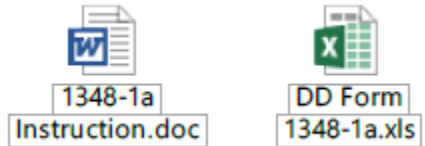


g. After you have removed the SSD card, replace the CAC reader, using the 3 screws from Step c, replace the black film tape.

h. This part of the process will take about 4 minutes give or take.

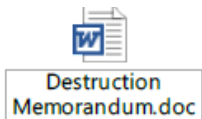
A-4. Instructions for filling out the DD 1348-1A and Memorandum.

a. Please follow the embedded instruction from DLA.mil for filling out the DD 1348-1A (embedded)



b. Fill out the embedded Memorandum. If you are going to send the SSD card to USAREC for destruction, then you need to send the SSD card with the memorandum to the following Address:

ATTN:
USAREC HQ G-6 Cybersecurity
1307 3rd Ave Ft. Knox, KY 40121



Appendix B

Guide to verify if Apps are approved for download and Requesting Mobile Apps through USAREC Cybersecurity.

Section 1. Introduction

B-1. Purpose

This guide provides the standard administrative procedures for verifying if the App you want to install on your government-issued smart phone is approved, as well as the standard administrative procedures for requesting new smart phone App's for USAREC Cyber approval and use.

B-2. References

AR 25-1 Army Information Technology

USAREC PAM 25-1-1 USAREC Information Technology Implementation Instructions USAREC 25-1 US Army Recruiting Command Information Technology

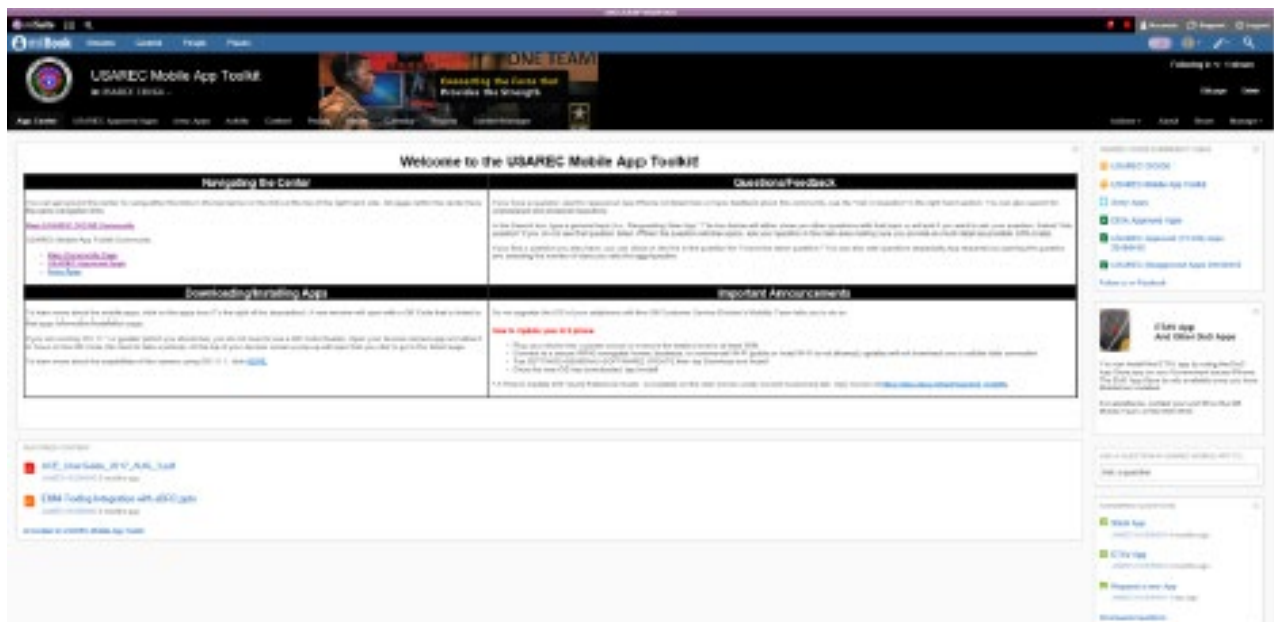
B-3. Responsibilities

Cybersecurity is a holistic program to manage information technology-rated security risk and to be effective it must be integrated fully into every aspect of the Command. It requires the implementation and enforcement of proper management and operation procedures by the entire organization. Furthermore, each individual, at every level, is responsible for procedural compliance with the proper practices and procedures for safeguarding information and IT. The responsibility for ensuring that personnel abide by these practices and procedures is inherent with Commanders and senior leaders of agencies and activities.

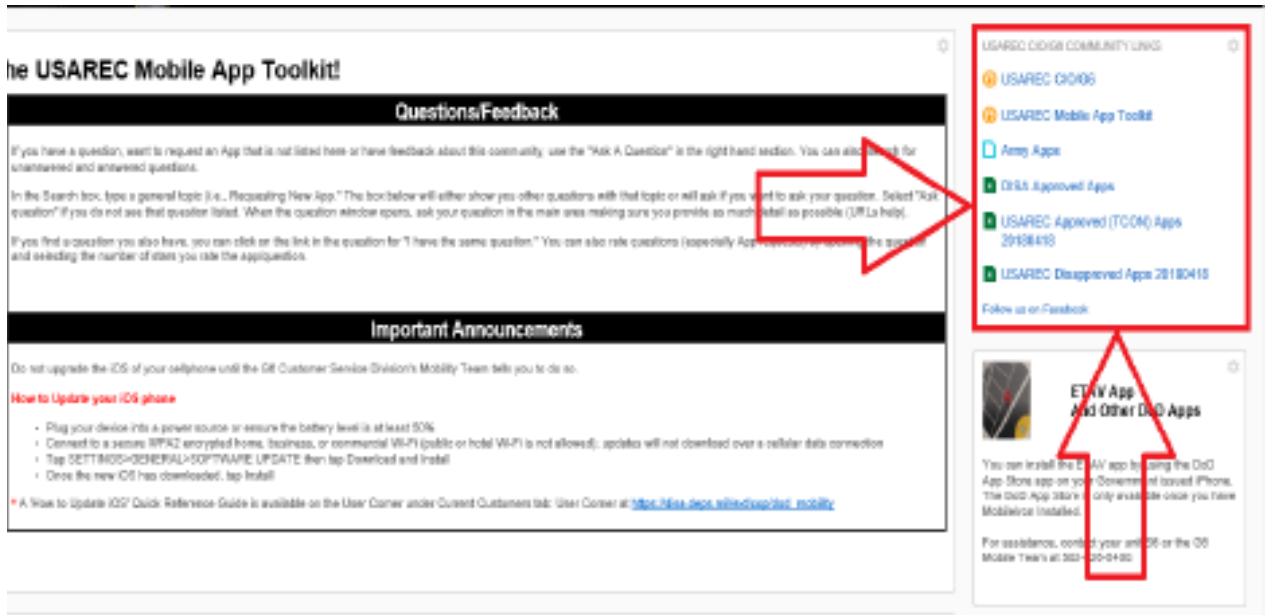
Section 2. Instructions

B-4. Verifying the App is Approve for Use.

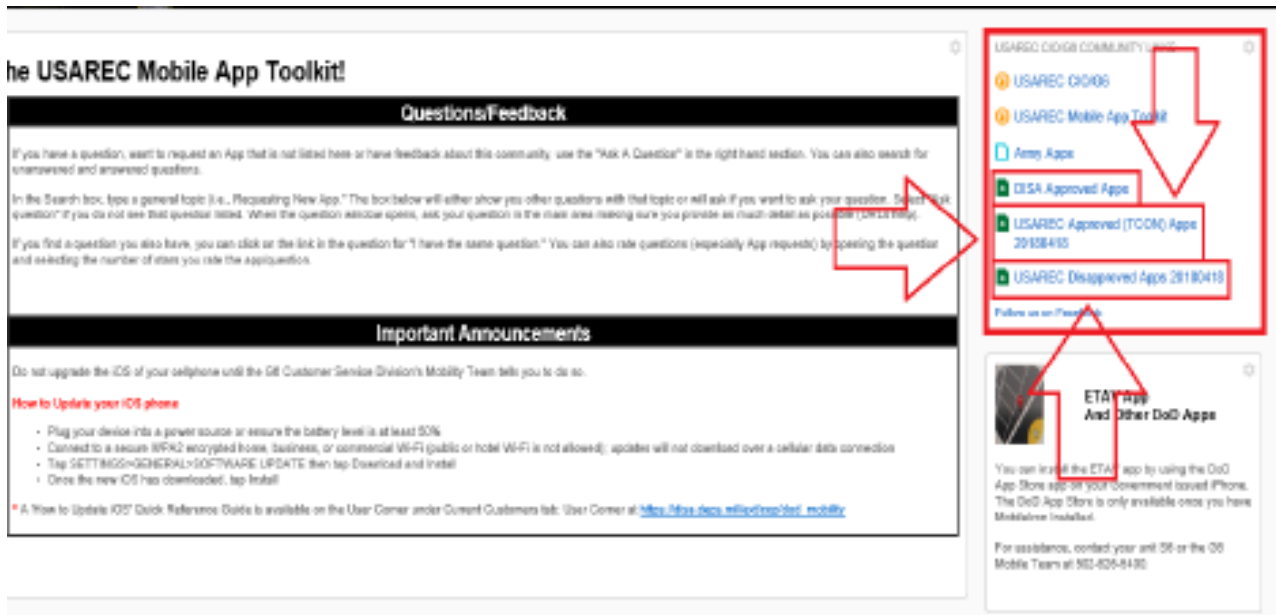
- a. Navigate to the USAREC Cyber managed webpage USAREC Mobile App Toolkit located in MilSuite at: <https://www.milsuite.mil/book/community/spaces/apf/usarec-G-6/usarec-mobile-app-toolkit>.



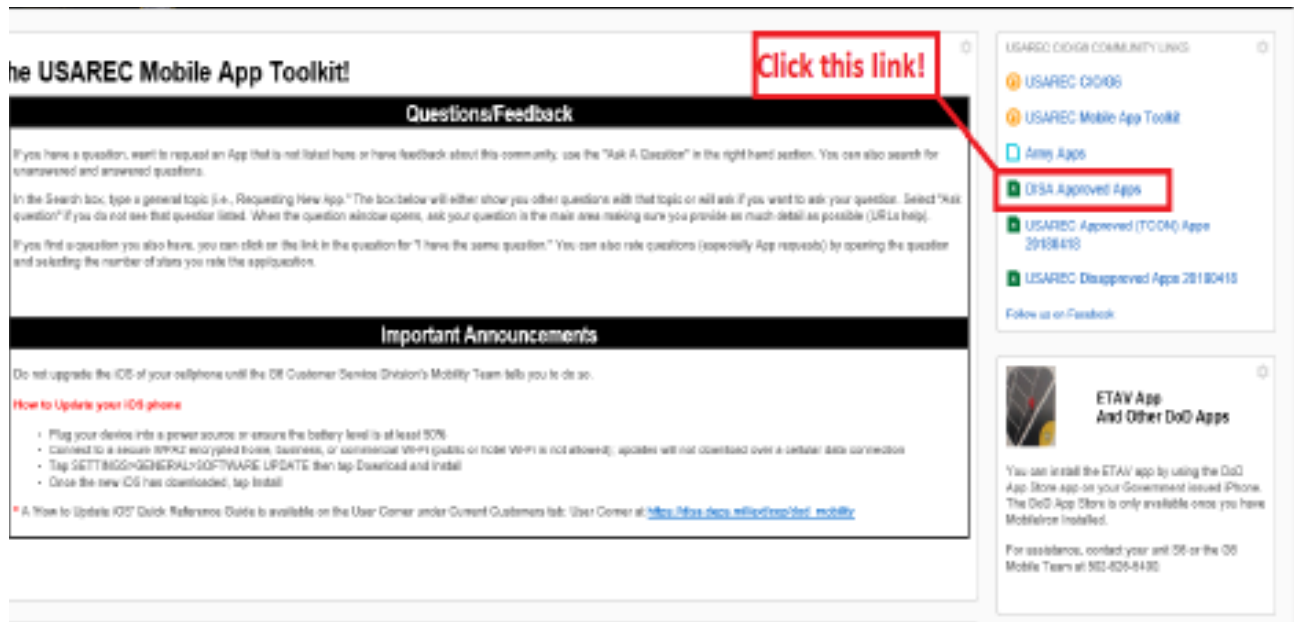
- b. Once on the USAREC Mobile App Toolkit website, you will navigate to the right side panel under USAREC CIO/G-6 Community Link



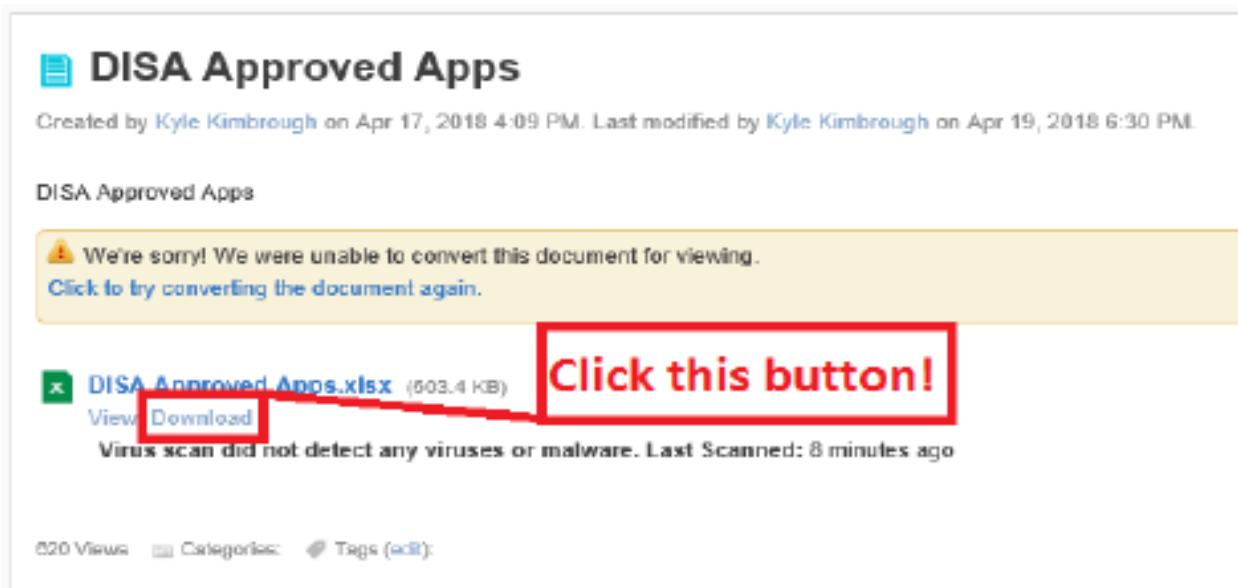
c. Under this side panel, there are three links to excel documents: DISA Approved Apps, USAREC Approved (TCOM) Apps YYYYMMDD, and USAREC Disapproved Apps YYYYMMDD



d. The first excel document is the DISA Approved Apps. This excel documents consist of all Apps that have already been approved by DISA. Click the Link.



e. Once you have clicked the excel document, you will be taken to the webpage. On this page you will normally receive a preview of the document (this particular document is rather large, so you might receive an error as you will see in the screenshot, ignore it). To view the document click the download button.



f. After clicking download you will be prompted for an Open/Save Prompt at the bottom of your screen, click Open.



g. After clicking Open, the DISA Approved Apps excel document will open in Excel. You can now search for all Apps that have been approved by DISA. If you find an App within this Excel document, then it's already approved and you can download it.

h. You can repeat steps "d" through "f" to open the USAREC Approved (TCON) Apps YYYYMMDD and the USAREC Disapproved Apps YYYYMMDD. The difference between the DISA Approved Apps Excel document, and the other two Excel documents, is when you reach step "e" you will see a preview because these Excel files are much smaller.

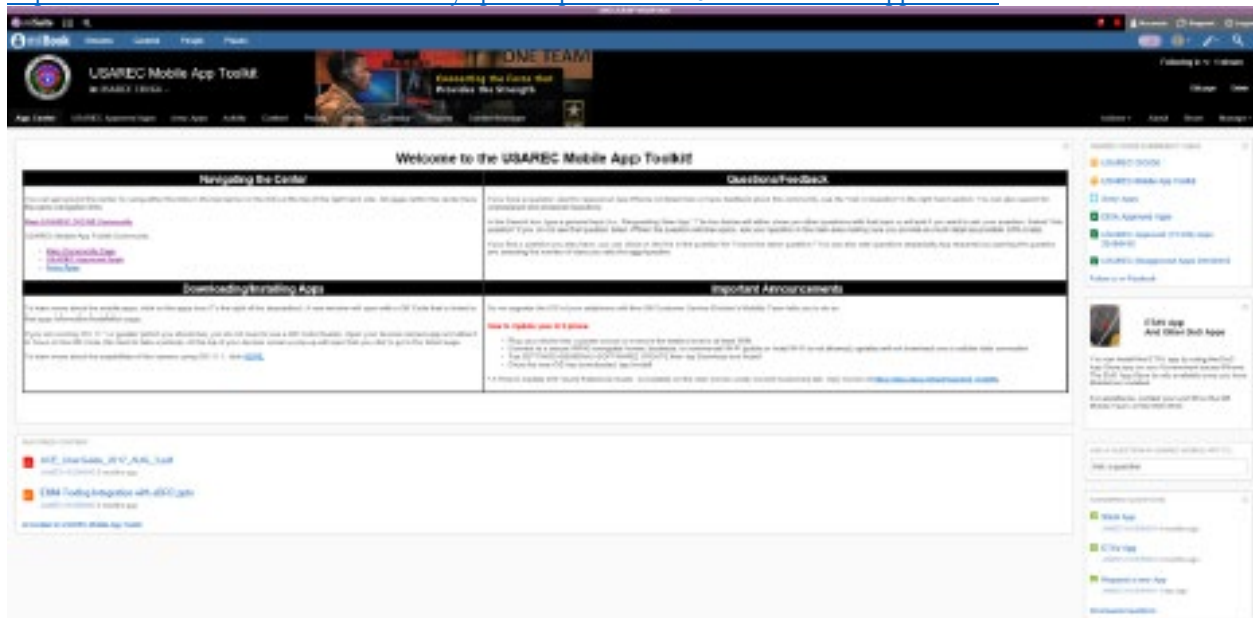
i. The USAREC Approved (TCON) Apps Excel document consists of all the Apps that USAREC Cyber has reviewed and approved for download and use on your government-issued smart phone. Most Apps on this Excel document will show as "Valid for 1 year unless otherwise disapproved by DISA". This simple means that USAREC Cyber has submitted a request to DISA for further review and approval. Apps that show as "Approved by DISA" means it was submitted to DISA and approved for use. If you have questions regarding Apps on this spreadsheet, feel free to contact USAREC Cyber at usarmy.knox.usarec.list.hq-G-6-ia-office-mgr@mail.mil.

j. The USAREC Disapproved Apps Excel document consists of all the Apps that USAREC Cyber has reviewed and disapproved for download and use on your government-issued smart phone. Each App on this spreadsheet will have a reason for why it was disapproved; those reasons can vary and could be subject to change. An example of change would consist of USAREC Cyber disapproving an App request, but further down the line DISA approves that same App, in such a case like that the App would then be moved to the USAREC Approved App spreadsheet and could then be downloaded for use. If you have questions regarding Apps on this spreadsheet, feel free to contact USAREC Cyber at usarmy.knox.usarec.list.hq-G-6-ia-office-mgr@mail.mil.

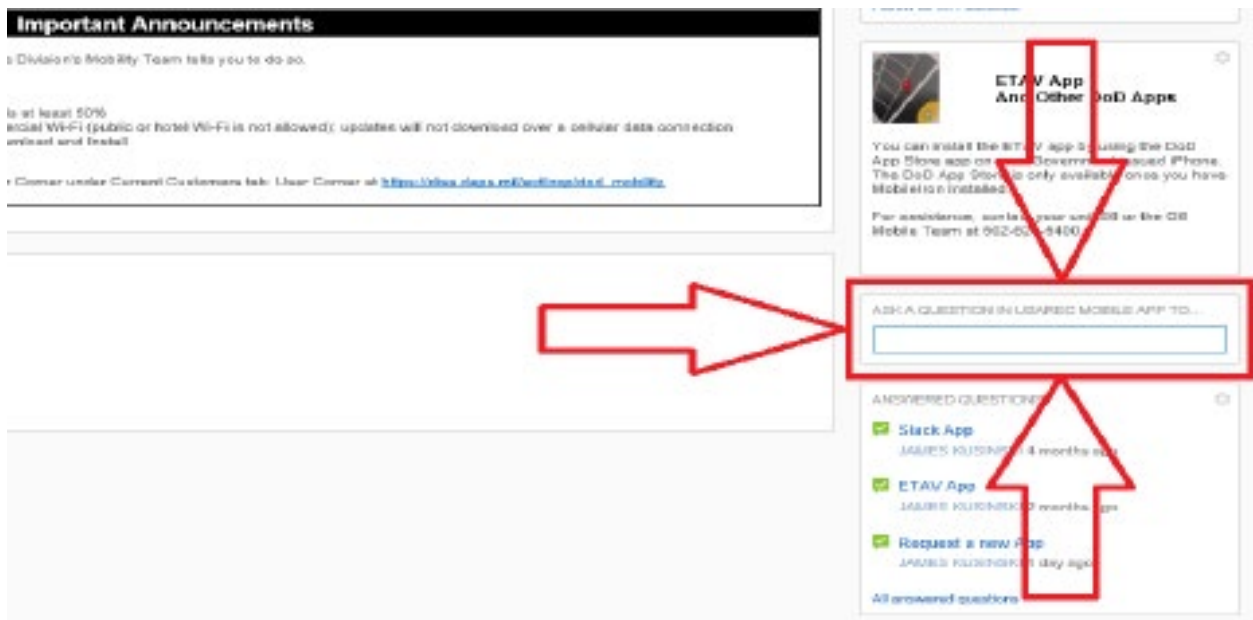
k. Apps on the DISA Approved spreadsheet or on the USAREC Approved (TCON) spreadsheet are approved for use. DO NOT download any Apps that are on the USAREC Disapproved Apps spreadsheet. Doing so could result in your phone being suspended or worse remotely wiped. If you find Apps approved by DISA, which are marked Disapproved by USAREC, if you find any mistakes on the spreadsheets please contact USAREC Cyber at the above email and let us know. These spreadsheets will be updated on a weekly basis.

B-5. Requesting a New App for Review and Use

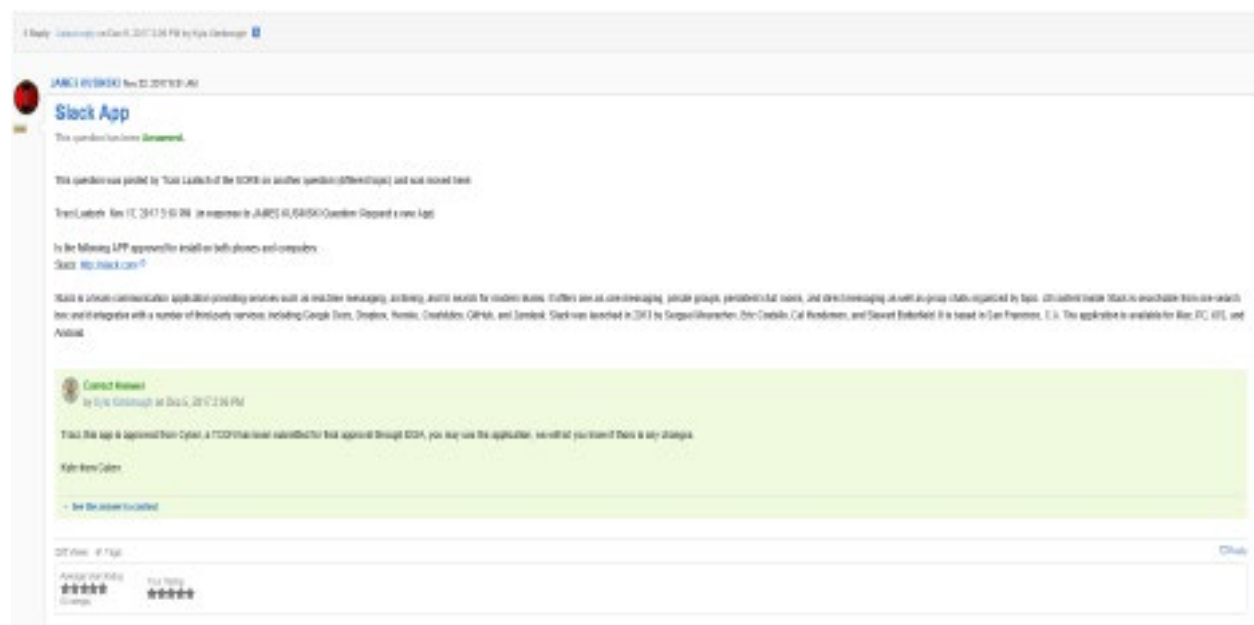
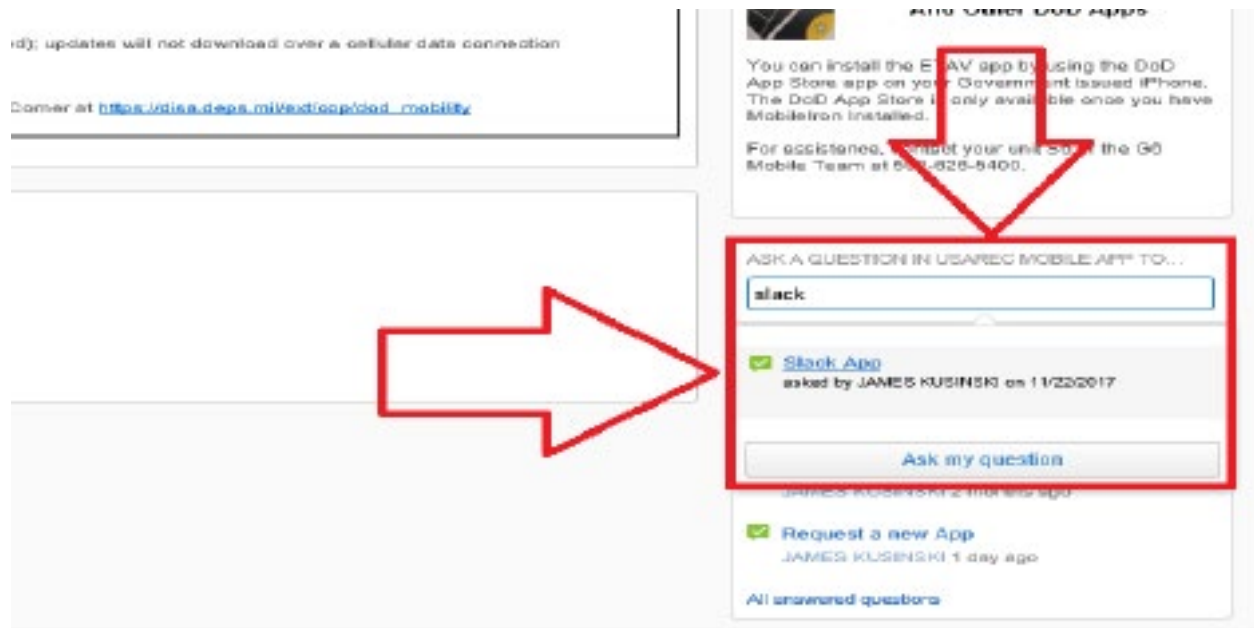
a. Navigate to the USAREC Cyber managed webpage USAREC Mobile App Toolkit located in MilSuite at: <https://www.milsuite.mil/book/community/spaces/apf/usarec-G-6/usarec-mobile-app-toolkit>.



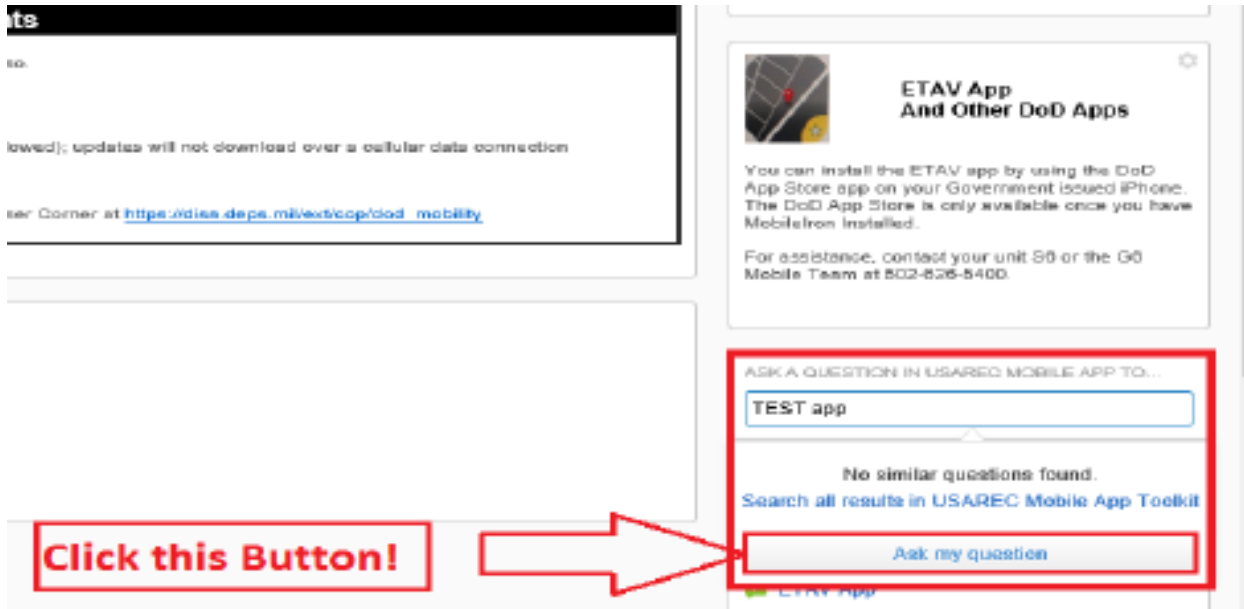
b. Once on the USAREC Mobile App Toolkit website, navigate to the right side panel under "Ask a Question in USAREC Mobile To."



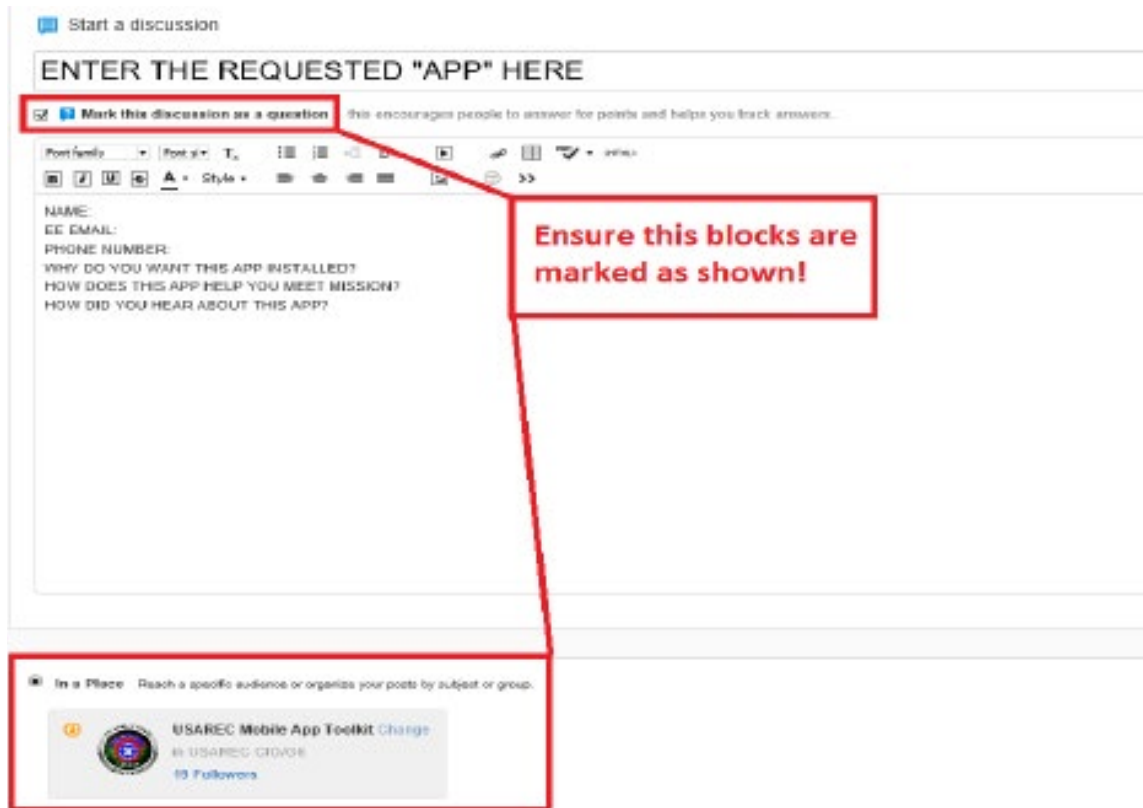
c. You can now ask a USAREC Cyber requesting a new App. You will notice as you begin typing in the box that if your response generates a similar question then you will be able to select that previously asked question and review the response (someone could already have requested that App so you can review the previous answer, and this will also help USAREC Cyber manage the questions better).



d. You will again notice as you begin typing in the box that if your response does not generate a similar question then you will be prompted with a message saying “No similar questions found”. This is where you can select “Ask my Question”.



e. After clicking the “Ask my Question” button, you will be brought to a screen to begin your discussion. As you will see in the screenshot below, you will need to leave the check mark in “Mark this discussion as a Question” block, and ensure the radio button “In a place” is selected, with USAREC Mobile App Toolkit being the group (should be default).



f. As for the Question, you will need to enter the App as the Title of the discussion such “Test App”. Then you will need to answer the following questions as seen in the screenshot below:

- 1) Name
- 2) Enterprise Email
- 3) Phone Number
- 4) Why do you want this App installed?
- 5) How does this App help you meet mission?
- 6) How did you hear about this App?
- 7) Each question needs to be answered.

The screenshot shows a web interface for starting a discussion. At the top, there is a button labeled "Start a discussion". Below it, a red-bordered box contains the text "ENTER THE REQUESTED 'APP' HERE". Underneath, there is a checkbox labeled "Mark this discussion as a question - this encourages people to answer for points and helps you track answers." Below this is a rich text editor toolbar with various icons for text formatting and alignment. The main text area contains the following text: "NAME:", "EE EMAIL:", "PHONE NUMBER:", "WHY DO YOU WANT THE APP INSTALLED?", "HOW DOES THIS APP HELP YOU MEET MISSION?", and "HOW DID YOU HEAR ABOUT THIS APP?". Below the text area is a large empty box for additional comments. At the bottom of the form, there is a section for "Go to PROCs" with a sub-section for "USAREC Mobile App Toolkit Change" which includes a profile picture, the name "USAREC GROUP", and a "Followers" count.

g. USAREC Cyber will check this page several times a day. Requests will be worked as we receive them. Please note that filling out your contact information is important because it allows us to give you a response for our decision on the App. We will reply in the post, but we will also email you with our findings. If you have any questions regarding this procedure or anything involving a Mobile App please don't hesitate to contact USAREC Cyber at usarmy.knox.usarec.list.hq-G-6-ia-office-mgr@mail.mil.

Glossary
Section I
Abbreviations

ABS

Accessions Baseline System

ACL

Access Control List

AGM

Army Gold Master

AIS

Army Information Systems

AMO

Acquisition Management Objective

AO

Action Officer

ARIMS

Army Records Information Management System

ATCTS

Army Training and Certification Tracking System

AUP

Acceptable Use Policy

BDE

Brigade

BN

Battalion

BOI

Basis of Issue

BOIP

Basis of Issue Plan

BPQ

Business Process Questionnaire

C4

Command, Control, Communications and Computer

CAC

Common Access Card

CATS

Case Adjudication Tracking System

CCF

Central Clearance Facility

COC

Command Operation Center

COI

Center of Influence

COR

Contracting Officer Representative

CoS

Chief of Staff

CPAC

Civilian Personnel Advisory Center

DEE

Defense Enterprise Email

DISA

Defense Information Systems Agency

DMDC

Defense Manpower Data Center

DOD

Department of Defense

DODIN

DOD Information Network

EUT

Early User Test

FBI

Federal Bureau of Investigations

FBI CJIS

Federal Bureau of Investigations Criminal Justice Information Services Division

FDO

Facilities Development Overview

FED

Federal

FOIA

Freedom of Information Act

FMO

Forms Management Officer

FP

Finger Prints

HQDA

Headquarters Department of the Army

HRC

Human Resources Command

HSS

Headquarters Support System

HW

Hardware

IA

Information Assurance

IAM

Information Assurance Management

IDA

Initial Denial Authority

IM

Information Management

IMS

Information Management Systems

IO

Investigating Officer

IT

Information Technology

ITAM

IT Asset Management Program

ITEP

IT Hardware and Software Request Form

MEPS

Military Entrance Processing Center

MTT

Mobile Training Team

MWNS

Mass Warning Notification System

NDA

Non-Disclosure Agreement

NOC

Network Operations Center

NPE

Non Person Entity

OGC

Office of General Council

OPM

Office of Personnel Management

OPSEC

Operational Security

OSJA

Office of the Staff Judge Advocate

PAA

Privileged Access Agreement

PAE

Positioning, Analysis and Evaluation

PBAC

Program Budget Advisory Committee

PCO

Publications Control Officer

PII

Personally Identifiable Information

PIPS

Personnel Investigations Processing System

PO

Print Order

POM

Program Objective Memorandum

PPBE

Planning, Programming, Budgeting, and Execution

PSI COE

Personnel Security Investigations Center of Excellence

RA

Registration Authority

REQUEST

Recruit Quota System

RFO

Reason for Outage

ROM

Rough Order of Magnitude

RSID

Recruiting Station Identification

RSN

Recruiting Services Network

SAAR

System Authorization Access Request

SME

Subject Matter Expert

SP

SharePoint

SW

Software

TASS

Trusted Associate Sponsorship System

TCO

Telecommunications Control Officer

TRADOC

Training and Doctrine Command

UFR

Unfunded Requirement

USAREC

United States Army Recruiting Command

VTE

Virtual Training Environment

Section II.**Terms**

There are no entries in this section.

USAREC

ELECTRONIC PUBLISHING SYSTEM

DATE: 1 October 2018
DOCUMENT: USAREC PAM 25-1-1
SECURITY: UNCLASSIFIED
DOC STATUS: ADMINISTRATIVE REVISION