

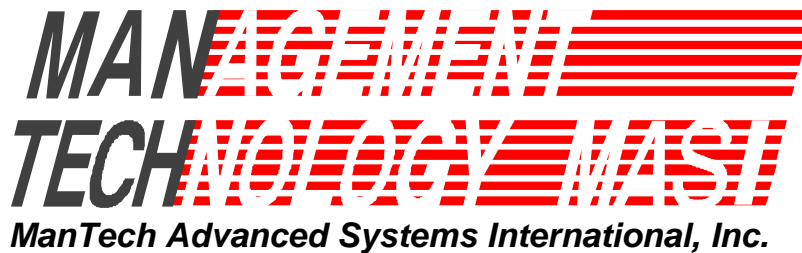
**FINAL
CONCEPT OF OPERATIONS
FOR A TYPE DESIGNATION
AUTOMATED SYSTEM
DOD CALS IDE PROJECT**

January 30, 1998

**Submitted by
ManTech Advanced Systems International, Inc.
West Virginia Technology Applications Operations Center
1000 Technology Drive, Suite 3310
Fairmont, West Virginia 26554**

**In support of
Contract DASW01-97-D-0006**

Non-CDRL



Robert S. Kidwell
Technical Director
DoD CALS IDE Project

Jack G. Richman
Project Manager
DoD CALS IDE Project

TABLE OF CONTENTS

LIST OF FIGURES	iv
LIST OF TABLES.....	v
1.0 SCOPE OF THIS DOCUMENT	1
2.0 BACKGROUND.....	2
3.0 OVERVIEW OF CURRENT PROCESS	5
3.1 Overcoming Inefficiencies in the Current Process.....	7
4.0 CONCEPT OF OPERATION	9
4.1 Objective	9
4.2 Requirements.....	9
4.3 Scope of TDAS	9
4.4 Constraints	9
4.5 Operational Environment	10
4.5.1 The Client/Server Architecture	12
4.5.2 WWW/Internet Computing.....	12
4.5.3 Hardware and Software.....	13
4.5.3.1 Server.....	13
4.5.3.2 Client-Contractors, Government Agencies, and Department Control Points	14
4.5.3.3 DoD Control Point.....	15
4.5.3.4 Telecommunication.....	15
5.0 OPERATIONAL SCENARIOS	16
5.1 TDAS Client View (Contractors and Department Control Point/Government Agency)16	
5.1.1 Submittal of DD Form 61(s).....	16
5.1.2 Manufacturing Contractor Functional Description	17
5.1.3 Administrative Contractor Functional Description.....	18
5.1.4 Department Control Points/Government Agency Pre-approval of DD Form 61.....	19
5.1.5 Department Control Point/Government Agency Functional Description....	19
5.1.6 Data Inquiry for Clients	20
5.2 TDAS DoD Control Point View	20
5.2.1 Approval and Update of DD Form 61(s).....	21
5.2.2 DoD Control Point Functional Description	21
5.2.3 Data Inquiry	22
5.2.4 Tracking.....	22
5.2.5 Report Generation.....	23
6.0 ANALYSIS OF THE SYSTEM.....	24
6.1 Summary of Advantages	24
6.2 Alternatives and Trade-offs Considered.....	24
6.2.1 TDAS Server Hardware	25
6.2.2 Web Application Development	25
7.0 TDAS IMPLEMENTATION ISSUES	26
7.1 Legacy Data	26
7.2 The DLSC Information Hub.....	27

7.3 EDA/SQL.....	28
7.4 Security	28
7.4.1 User Authentication.....	28
7.4.1.1 Stand-alone Application in a Network Environment	29
7.4.1.2 World Wide Web Based Application in a Network Environment	29
7.4.2 Database-Level Security	30
7.4.3 Internet Security.....	30
7.4.3.1 Virus Detection, Identification, and Eradication	30
7.4.3.2 Firewalls	31
7.4.3.3 SOCK Network	32
7.4.3.4 Public Key Cryptography (PKC)	32
7.4.3.5 Secure Socket Layer	33
7.4.3.6 Oracle Advanced Networking Option.....	34
7.4.3.7 Virtual Private Data Networks and Point-to-Point Tunneling Protocol	35
7.4.4 Security Audits for Windows NT 4.0 Servers	36
7.5 Database Schema Design	37
7.6 TDAS Help Design.....	37
APPENDIX A: REFERENCES	A-1
APPENDIX B: ACRONYMS AND ABBREVIATIONS	B-1
APPENDIX C: GLOSSARY	C-1
APPENDIX D: FUNCTIONAL FLOWS	D-1

LIST OF FIGURES

Figure 2.0-1 The DLSC Information Hub Concept	3
Figure 3.0-1 Existing Type Designation Process Flow at CECOM.....	6
Figure 4.5-1 System Architecture	10
Figure 4.5-2 Form DD61 Form Submission Process Tiers.....	11

LIST OF TABLES

Table 5.0-1 TDAS Action Command Matrix for Various Users	16
Table 5.2.4-1 TDAS Report Command Matrix for Various Users.....	23

1.0 SCOPE OF THIS DOCUMENT

This “Concept of Operations” (CONOPs) for a Type Designation Automated System (TDAS), is the third release and is designated as the “final” report. The final release contains updated information, as well as process and functionality flow charts for the TDAS. This report provides project background information in Section 2.0, while Section 3.0 describes the current type designation process and how an automated system can overcome inefficiencies in this process. The objective, requirements, scope, constraints, and assumptions, as well as the “concept of operations” are described in Section 4.0. A series of operational scenarios of the TDAS are discussed in Section 5.0. An analysis of the TDAS system is discussed in Section 6.0. Implementation issues regarding legacy data, security, the Defense Logistics Service Center (DLSC) information hub, Enterprise Data Access (EDA)/Structured Query Language (SQL), and database design are addressed in Section 7.0. Charts depicting the system’s functional flow for the automated system are provided in Appendix D.

2.0 BACKGROUND

The DLSC supports defense-system procurement by assigning, tracking, and retiring National Stock Numbers (NSNs) for all equipment used by the Department of Defense (DoD). DLSC maintains a database, the Federal Logistics Information System (FLIS), relating each NSN to information about the appropriate item. The assignment of a single NSN prevents duplication and unnecessary stock and storage of items. In addition to NSNs, the FLIS contains information including item names, characteristics information, interchangeability and substitutability data, hazardous-material disposal codes, demilitarization data, unit pricing, manufacturer's part numbers, and much more. DLSC supports all logistics functions of the DoD, other Government agencies and foreign governments through the collection, processing, storage, and dissemination of this data. DLSC uses the FLIS as the primary means to organize and maintain information from the Federal Catalog System. The NSNs are assigned by DLSC at Battle Creek, Michigan based on requests from the armed-services branch using the item.

The request for NSNs often comes from military service type designation organizations such as the U.S. Army's Communication and Electronic Command (CECOM) and the Air Force Material Command (AFMC). Each of these organizations has a system (a Military Service Type Designation System or MSTDS) of standards for naming and codifying equipment according to a type designation that specifies the *installation*, *equipment type*, and *purpose* of the item. A type designation is assigned for each item used by the U.S. Military Services. The request for an NSN assignment to DLSC comes after the type designation has been assigned.

DLSC, CECOM, and AFMC share some common information such as type designation, drawing number, and part number. Although this is a duplication of information, at present, contractors and Government personnel often have to work with all these organizations to find information relevant to systems or equipment they are provisioning, developing, modifying, repairing, and so on. In fact, if the inquirer does not know the exact organization involved with the equipment then relevant information will be missed altogether. These conditions exist because there is no direct connectivity between the various MSTDSs and between the MSTDSs and DLSC. Each exists as an independent system with only loose, and usually manual, ties to the others. According to DLSC, this lack of connectivity contributes to the duplication of acquisition and logistics efforts, the inability to find parts in inventories, the duplication of parts in inventories, and numerous other logistics management issues.

In order to address this lack of connectivity, DLSC has proposed that an automated system be established, the DLSC information hub, which will allow access to parts information in the FLIS and MSTDSs through a single user-interface. (See Figure 2.0-1.) This system would allow a user to enter certain key information (e.g., a part number or type designation) and discover which systems have information on a part and what the information is. Thus, all information on a part would be available to a DLSC user and the problems discussed above would be alleviated.

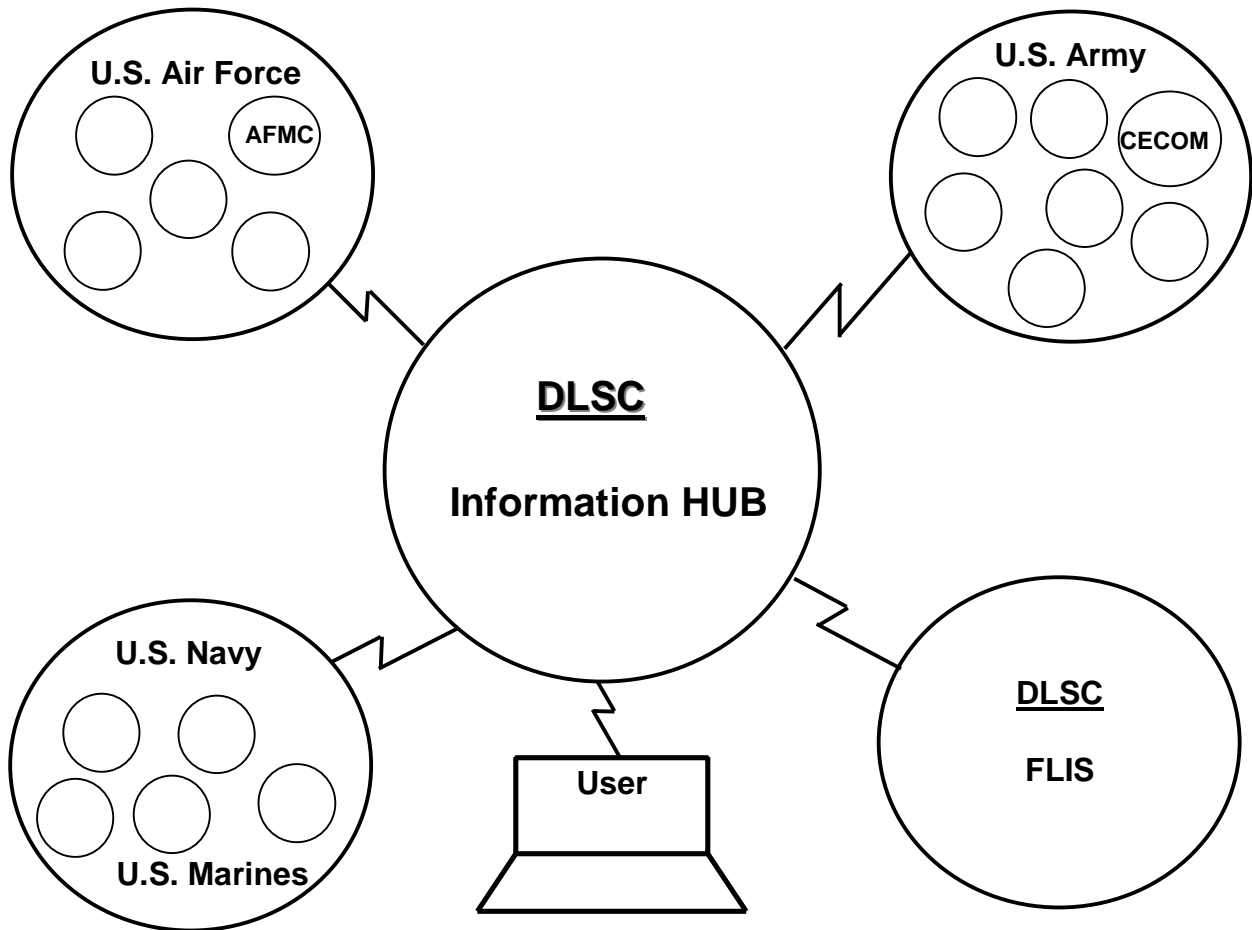


Figure 2.0-1 The DLSC Information Hub Concept

Task 2 of the Continuous Acquisition and Life-cycle Support (CALs)/Integrated Data Environment (IDE) program (Contract No. DEAM21-96-MC32239) was tasked with assessing the client/server architecture proposed by DLSC for the DLSC information hub and the capability of the existing type designation systems at CECOM and AFMC to participate in this architecture. Task 2 was initiated with the understanding that CECOM and AFMC had some type of automated type designation system in place. Unfortunately, it was found that neither CECOM nor AFMC have automated MSTDSs. No complete, computer resident database or computer-readable database exists. CECOM and AFMC each keep a small dBase III database for tracking DD Form 61 requests as they come in. The DD Form 61 is the standard form that must be submitted to an MSTDS for type designation. The two databases share only a few common data fields, contain only a small subset of DD Form 61 data, contain much data not on DD Form 61s, and have been in use for only a few years.

Beside this tracking database, CECOM has no automation for type designation. AFMC, however, uses a Canonfile 250 image scanner to scan and store DD Form 61s to optical disks. These disks can then be read by a Canon Diskfile Drive 5001S with CFView software for viewing and manipulating the DD Form 61 images on any IBM-compatible PC. AFMC has used this

equipment since 1987 for all DD Form 61s. As a courtesy, they have provided Canonfile disk copies to CECOM for the DD Form 61s that are sent from the United States Air Force (USAF) to CECOM for processing. Beyond this use of the Canonfile equipment and the tracking database, there is no automation of the type-designation process. Further detail on the analysis of the environment at CECOM and AFMC appears in the report "Preliminary Military Type Designator Systems Assessment for the DoD CALS IDE Project" January 1997, Contract Data Requirements List (CDRL) sequence numbers A005.

The result of an analysis of CECOM and AFMC was to determine "the degree to which the CECOM and AFMC type designation systems need to be augmented" in order to participate in the DLSC client/server architecture. Unfortunately, it was discovered that the "degree of augmentation needed" could be summarized as follows:

No automated MSTDS exists at CECOM or AFMC that can take advantage of the proposed DLSC architecture. Thus, there is currently nothing to augment. Before CECOM or AFMC can participate in the DLSC hub concept, their MSTDS must be automated.

Building these systems was not envisioned when the contract was undertaken. However, after all parties understood the real state of the CECOM and AFMC systems, it was agreed to undertake an effort to work with CECOM and AFMC to develop the necessary automated systems. This work is beyond the original scope of the contract, but meets the real needs of the DoD CALS community, CECOM, and AFMC.

In order that all parties understand the proposed automated system to be built for CECOM and AFMC, this non-CDRL document will explain the Concept of Operations for a TDAS. Since the challenges faced by MSTDS personnel at CECOM and their users are greater, the TDAS system will first be developed for and deployed at CECOM. Close contact is being maintained with AFMC so that the resultant TDAS will also meet the needs of AFMC without substantial modification.

3.0 OVERVIEW OF CURRENT PROCESS

The process for the MSTDSs in place at CECOM and AFMC is not automated. The current process for assigning a type designation within CECOM is sequential as illustrated in the process flow diagram, Figure 3.0-1. Please keep in mind that CECOM serves as both the Department Control Point (DCP), (referred to as the pre-approval point below), and the DoD Control Point. CECOM's architecture is a three tier implementation as explained in later sections.

1. The Manufacturing Contractor (customer) prepares and mails DD Form 61(s) to the Department Control Point. The contractor may mail one or a group (see "package" in glossary) of DD Form 61(s). The latter occurs when a system with new parts is being nomenclatured.
2. Department Control Point personnel receive DD Form 61(s) and quickly screen the form(s) for apparent errors and correct number of copies. DD Form 61s may be rejected and sent back to the contractor at this point, if errors are severe.
3. DD Form 61(s) are retrieved for working according to the oldest date received and a further validation of data is begun by the Department Control Point personnel.
4. If there are minor errors then the contractor responsible for the DD Form 61(s) is contacted, problems are resolved, and the process continues. If there are severe errors, the contractor is notified and asked to send a corrected form.
5. The Department Control Point personnel verify that all necessary data is present, in correct format and there are no conflicting data fields.
6. The Department Control Point personnel assign a Source Request Number (SRN) (see "SRN" in glossary) for each item and sign and date the DD Form 61(s).
7. Department Control Point prepares and mails DD Form 61(s) to the CECOM. The Department Control Point may mail one or a group of DD Form 61(s).
8. CECOM personnel receive DD Form 61(s) and quickly screen the form(s) for apparent errors (such as a missing SRN) and correct number of copies. DD Form 61(s) may be rejected and sent back to the Department Control Point at this time, if errors are severe.
9. Tracking data (e.g., date received, source request number, etc.) is entered into the dBase III tracking database.
10. The paper DD Form 61 is either stored in a file cabinet for later working (CECOM) or scanned into the Canonfile 250 (AFMC).
11. DD Form 61(s) are retrieved for working according to the oldest date received and a further validation of data is begun by the CECOM personnel.
12. If there are minor errors, then the Department Control Point responsible for the DD Form 61 is contacted, problems are resolved, and the process continues. If there are severe errors, the DD Form 61 is sent back to the Department Control Point with an error report explaining what needs to be corrected. The Department Control Point would then correct the problems by the contractor or by sending back the form to the contractor to be sent through the process again.

Existing Process Flow

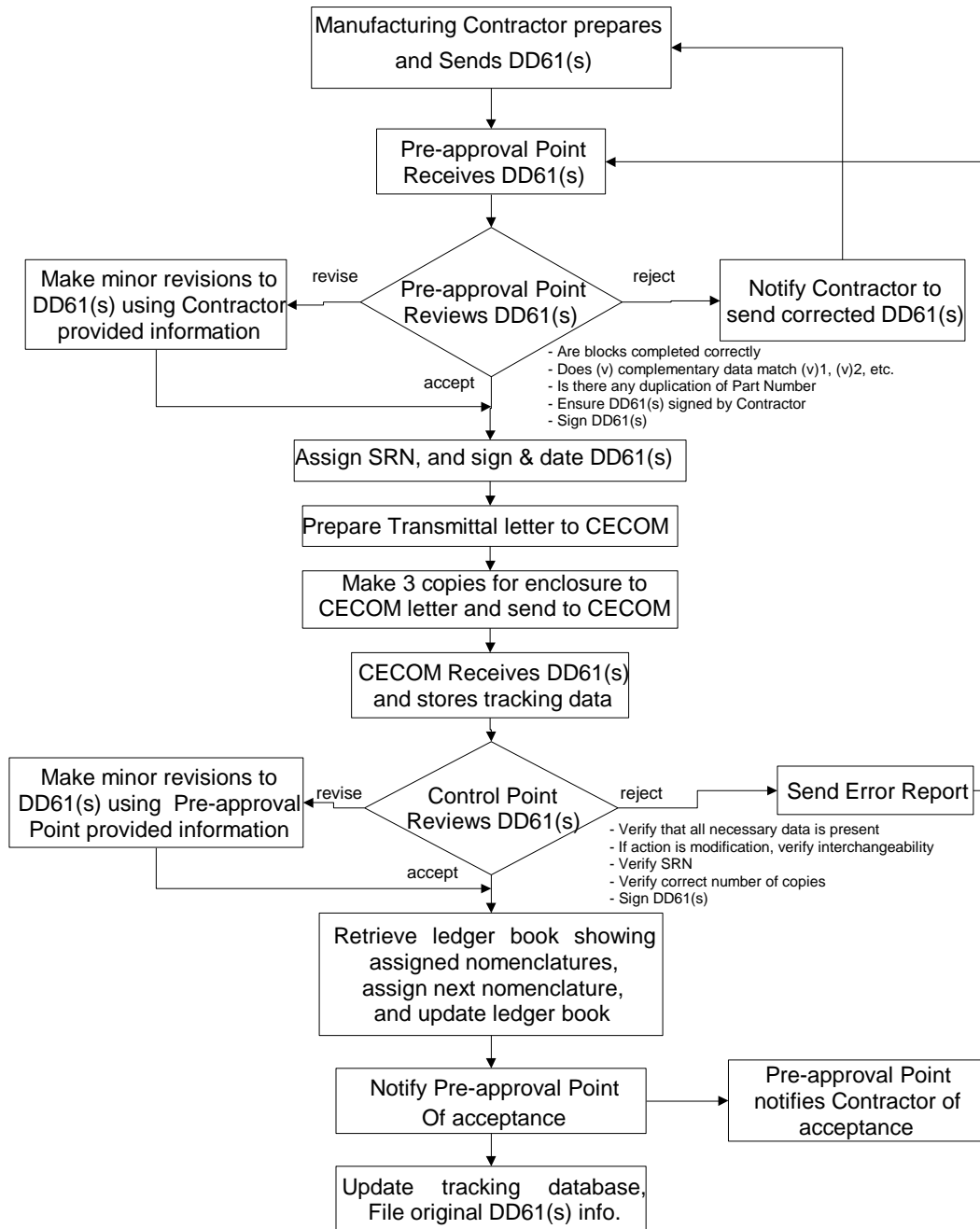


Figure 3.0-1 Existing Type Designation Process Flow at CECOM

13. The CECOM personnel verify that all necessary data is present, in the correct format and that there are no conflicting data fields. (E.g., if the request is to assign a modification, there must be some indication of the degree of interchangeability between this and present models.)

14. The CECOM personnel retrieve a ledger book that shows all nomenclatures ever assigned at the CECOM.
15. The appropriate page is found for the requested item and the next nomenclature in the sequence is assigned on the original DD Form 61(s).
16. The ledger is updated to reflect the new nomenclature.
17. The DD Form 61 is sent to supervisory personnel for signatures. This action is largely perfunctory and is being removed.
18. A cover letter is prepared for the DD Form 61(s).
19. Copies are made of the letter and the completed DD Form 61(s). These are then sent to the Department Control Point (and from the Department Control Point on to the contractor) appropriate agencies in the Army or USAF, and to DLSC.
20. The tracking database is updated with information such as completion date and final nomenclature.
21. The original DD Form 61(s) and cover letter(s) are filed.

This is the basic process for assigning a new type designation. A revision or cancellation has some slight modification, but generally follows this basic process flow.

In addition to DD Form 61(s), CECOM and AFMC personnel must respond to customer requests for information. In some cases, especially for DD Form 61(s) that are in the process, this requires a lookup in the tracking database. However, often the request precedes a DD Form 61 submittal. At CECOM, this involves searching manually through forms, microfiche, and microfilm to find requested information. At AFMC, this involves searching through the Canonfile disks.

3.1 Overcoming Inefficiencies in the Current Process

Obviously, a manual process as described above has much inefficiency that can be improved by an automated system. First, there is the storage of the data. At present, CECOM data is simply stored as the actual paper DD Form 61(s) submitted. AFMC stores the DD Form 61(s) as Canonfile images. There is also some redundancy in that some data is kept on the dBase III tracking file and some in the ledger books. The paper and ledger books use substantially more storage space than an automated system. At present, storing in this medium means that someone must manually place the DD Form 61 copies in the appropriate location in a file cabinet. In the case of the ledger books, someone must write-in the correct subset of data. A single, automated system would remove the redundancy, reduce storage space, reduce the time to place into storage, and reduce the possibility of human errors in entering handwritten data.

Legacy data is currently stored in five media: paper DD Form 61(s), Canonfile images, microfiche, microfilm, and UNISYS tape reels in System 2000 (S2K) format. Some of the data in the same media is in different formats. This storage obviously takes up more space and is more difficult to manage than an automated system.

A second and related issue is that of the retrieval of data. At present, when CECOM receives a request for data, they must manually search for it. Even at AFMC, searching is not completely automated, for they must manually search through the images. After a search, CECOM or AFMC

mails the Department Control Point copies of the data, often many more copies than the Department Control Point needs. The Department Control Points and contractors must then search through the paper copies to find the data elements needed. Using an automated system, the customer will be able to directly query and retrieve only the data elements needed and in a much shorter time - minutes instead of days.

A third issue is the use of the mail to submit DD Form 61(s), send rejection notices, and notify completion to the Department Control Points, contractors, and appropriate agencies. This adds many days, possibly weeks in the case of a rejected and resubmitted DD Form 61, to the process. With an automated system, the contractor and then the Department Control Point can submit the DD Form 61 as soon as it is completed and it is immediately received at the MSTDS. Furthermore, the Department Control Points or contractors can be immediately notified if the MSTDS finds an error and can resubmit as soon as the error is corrected. The Department Control Points, contractors, and appropriate agencies can be notified immediately upon completion of a DD Form 61. Thus, automated submittal, rejection, and acceptance notification should greatly reduce the time it currently takes to process a DD Form 61.

Another activity, which takes a great deal of time and effort in the process, is the manual validation of the data on a DD Form 61. The MSTDS personnel must manually check every field to insure that there is data in the field, that it is in the appropriate format, and that the entry is logically possible for the type of request and the equipment being nomenclatured. Although not pointed out in the process outlined above, the requesting contractor must review the form before it is submitted. Much of this manual validation would be removed in an automated system. An automated system would ensure that there is data in all fields that must have entries, and that the data is in a correct format. Contractors, Department Control Points, and MSTDS personnel will not have to check for these types of errors. The only errors which will require manual validation are those which require expert judgment. For example, the requested item name would be logical if the type designation appears to be logical, given the type of request and equipment. Automated validation will save all personnel a great deal of time and will reduce the possibility of missing or incorrectly formatted data to near zero.

There is also some effort expended in checking for the appropriate number of copies and making copies to send. This effort would be greatly reduced since the contractors, Department Control Points, and MSTDS personnel, if needed, can create multiple copies via an automated request, send multiple copies, and attach copies to E-Mail.

Finally, the activity of assigning the nomenclature and updating the database will be enhanced. The MSTDS personnel will not have to access a ledger and find the appropriate page and nomenclature list, but will simply query the system based on critical data-elements (e.g., item name and type designation) to retrieve possible assignments. Once this change is made and any other changes to the DD Form 61 are final, the MSTDS personnel can update the database with a simple click on a screen or entry of a command. The appropriate DD Form 61 will then be updated as a final set of data in the TDAS database. Also, since security precautions will be taken, only the appropriate personnel can modify and update this data.

4.0 CONCEPT OF OPERATION

This section will provide information on the automated TDAS system requirements, hardware, software, architecture, and user communities.

4.1 Objective

The objective of this effort is to provide an automated system that will replace the current manual paper based MSTDS in use at sites such as CECOM. Additionally, the objective is to provide an infrastructure to facilitate the type designation process for the contractors of the site.

4.2 Requirements

The proposed TDAS will include, but not be limited to, the following top-level requirements:

1. Allow contractors to directly retrieve CECOM type designation data.
2. Allow MSTDS personnel to directly retrieve and update DD Form 61 data.
3. Enable electronic submittal of DD Form 61.
4. Facilitate contractor entry of appropriate data on DD Form 61.
5. Facilitate verification of appropriate data on DD Form 61 input.
6. Develop database of relevant DD Form 61 and previous type designation data.
7. Enable retrieval of legacy DD Form 61(s) via key fields in database.
8. Enable connectivity from the DLSC information hub.
9. Provide security to control access to DD Form 61 data.
10. Enable production of custom reports.

4.3 Scope of TDAS

The automated system, the “*TDAS*,” will enable electronic submittal of DD Form 61(s), inquiries to retrieve previous type designation data stored in the database within TDAS, and assignment of nomenclature. All the data submitted on the electronic DD Form 61(s) via TDAS will be stored within the TDAS database.

4.4 Constraints

TDAS will be designed to allow Transport Control Protocol (TCP)/Internet Protocol (IP) access to its functions. In addition, Information Builders, Inc. EDA/SQL software will be included to enable responses to the DLSC hub. Outside of these capabilities, TDAS will supply no other networking capabilities. These capabilities (all necessary network software and hardware) are to be provided by the sites in which TDAS is to be installed.

TDAS will function in a Windows NT client/server environment using an Oracle 7.3 Relational Database Management System (RDBMS). See the Operational Environment section (4.5) for more specific detail on the environment necessary to run TDAS.

4.5 Operational Environment

CECOM and AFMC personnel responsible for final processing of DD Form 61(s) (hereinafter, DoD Control Points or SuperClients below) will access the TDAS through Local Area Network (LAN) connections. External users who currently submit DD Form 61(s) through the mail will access the TDAS through the Internet. The preliminary system architecture is illustrated in Figure 4.5-1.

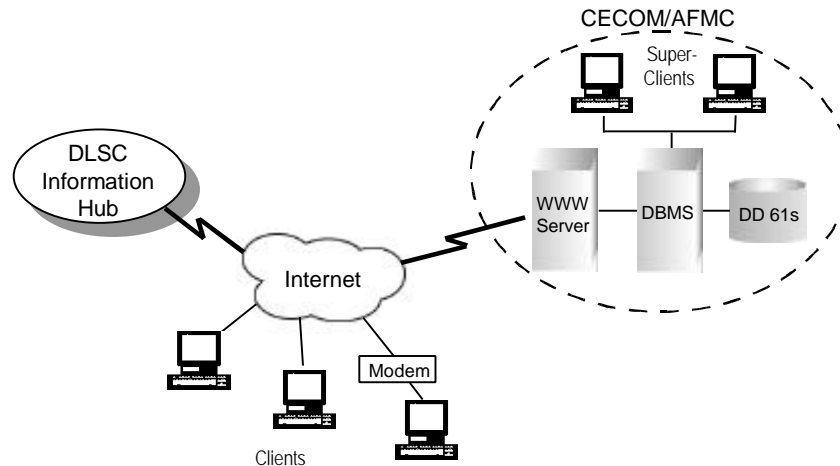


Figure 4.5-1 System Architecture

Two types of high-level users of TDAS have been identified: the DoD Control Points and clients. DoD Control Points are TDAS personnel who are responsible for DD Form 61(s) processing. Because they need to approve or reject DD Form 61 requests, generate various reports, and perform other tasks to support their day-to-day functionality, they will be given the highest level access to the database system.

DoD Control Points will have read/write privileges for all database contents. They will have a LAN/Wide Area Network (WAN) connection to the TDAS server.

Clients are those who submit DD Form 61 requests to the TDAS. There are three types of clients: Department Control Points, Government Agencies, and contractors.

Clients are composed of Contractors, Government Agencies, and Department Control Points. Different levels of functionality exist; however, no additional software or hardware is required to handle these differences. All three types are using a classical computer definition, "clients."

The client access level will be determined by CECOM/AFMC and will be given the appropriate permissions based on their respective username and password. Viewing (read) permission can be setup by CECOM/AFMC to control the client access and querying ability.

Clients

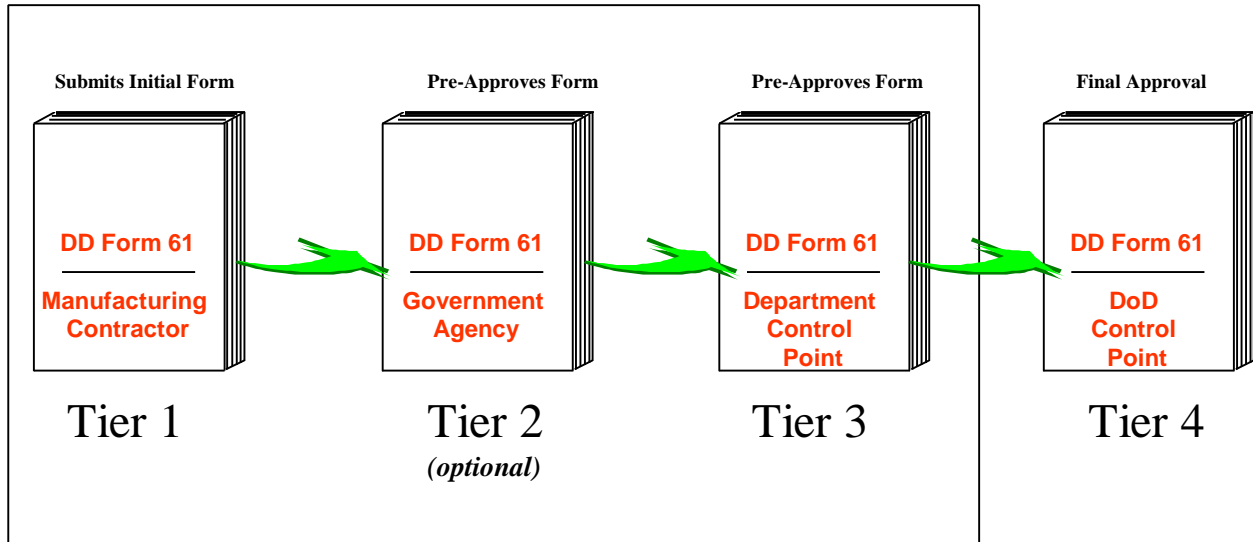


Figure 4.5-2 Form DD61 Form Submission Process Tiers

In the case of the ARMY, CECOM personnel serve as both the Department Control Point for the Army as well as the DoD Control Point. The ARMY architecture would essentially be a three tier system. However, the AFMC architecture would implement the 4th tier of the Government Agency.

Department Control Points will have the ability to retrieve the information submitted by the contractors. In some cases dependent on the particular defense agency, another level of approval is utilized with the submission process. This level will be referred to as a Government Agency as shown in figure 4.5-2 above. The Government Agency functionality will be identical to that of the Department Control Point. The Department Control Points will validate and finish the DD61 form before submitting it to the DoD Control Point for review. The Department Control Points and Government Agencies will also have the same query ability as the contractors.

Contractors will submit DD61 information to Government Agencies and/or Department Control Points for further submission to the TDAS personnel. In addition to the submittals, they often need to inquire about information from the type designation system regarding, for example, nomenclature, part number, or Commercial And Government Entity (CAGE) code. A contractor may submit information for review by a Government Agency/Department Control Point, for validation, and then it is sent on to the DoD Control Point for final approval. These users will be allowed to perform inquiries but not updates. Therefore, they will be given restricted access to the database. Contractors may consist of either manufacturing or administrative types. The manufacturing contractors may submit requests for type designation actions as directed by the procuring activity and their respective read privileges are determined and set according to the DoD Control Point's assignment of the account. In this document, the term contractor will refer to the functionality of a Manufacturing Contractor. An Administrative Contractor can (1) view a

particular image (DD61) or approved submittal and (2) request a report from all of the data but can not submit a DD Form61.

There are two types of contractors: manufacturing and administrative. Manufacturing can submit DD 61 forms and view what they have submitted; however, Administrative Contractors have only view privileges based on their assigned access level.

The DoD Control Point site (e.g., CECOM, AFMC) will determine who is allowed access and the privilege level that is appropriate.

4.5.1 The Client/Server Architecture

World Wide Web (WWW) computing can be categorized as client/server computing in which the Web server acts as server and the Web browser as client. However, the client/server architecture discussed in this section is the more traditional one that is operated in a LAN environment. The main components of this architecture are the Database Management System (DBMS) running on the TDAS server and two DoD Control Point workstations.

Client/server computing has been recognized as one of the new standards in the database applications arena. A typical, two-tier, client/server, database application is somewhat like a PC on a LAN. While the PC on a LAN asks for files from a file server, the client/server database application asks for data from a database server. The user-interface portions of the application run on a local PC and are separated from the data by a network cable and a database server. The front-end client portion runs on a local PC, while the back-end database engine runs on a database server. Thus, this arrangement takes advantage of distributed processing. Based upon the needs and requirements of the user community, a client/server system can be as simple as two-tier, three-tier (with an additional application server), or multi-tier architecture.

Advantages of client/server computing are summarized below:

- Better leveraging of emerging desktop computing technology.
- Reduction in Internet network traffic.
- Open system flexibility in the selections of both the front-end development tools and the back-end database server.
- Ease of training and user acceptance using a Graphical User Interface (GUI).
- Performance and scalability in improving query performance against large tables.
- Integrity and security because of the separation of the client application from the data.

4.5.2 WWW/Internet Computing

The use of the Internet as the framework upon which the TDAS will be built allows us to take advantage of the Internet capacity for graceful degradation. It was a desire for just such as bend-but-don't-break communications network that prompted the development of the Internet's precursors. Today, we can leverage both the research and development investment that the

Internet represents, and technological lessons learned in the course of its creation and subsequent exponential growth.

The most significant benefit of a WWW approach is the elimination of the physical software installation and configuration management problem. There would be a tremendous cost in terms of person-hours and money necessary to install software for hundreds of users of CECOM and AFMC. The process and cost would be repeated whenever there is any software update. Therefore, the WWW approach is attractive and cost-effective for supporting external clients.

4.5.3 Hardware and Software

After thorough analysis of CECOM's current process, initial TDAS hardware and software requirements have been identified. Although the requirements are mainly based on CECOM's needs and workload, they can be easily applied to the other MSTDSs since CECOM represents the largest workload (about 3,000 DD Form 61 requests per year) among all MSTDSs. Furthermore, because of the proposed open and scaleable approach, the final selection of hardware and software can be customized to meet each MSTDS's requirements without affecting the underlying architecture.

4.5.3.1 Server

One of the most critical components within this client/server architecture design is the TDAS server itself. This server will serve as a DBMS, as well as a Web server and will host the EDA/SQL server that is mandated by DLSC for the connection from the information hub. In light of our analysis, and given budgetary constraints, the following has been identified as the base for the server configuration.

Hardware

Based on performance and cost, the following server was selected:

- Advanced Logic Research (ALR) Revolution Quad6 Server
- 200 MHz Pentium Pro Symmetric Multi-Processor (SMP)
- 128 MB memory
- 18 gigabytes (GB) disk capacity
- 2 CPUs installed -- expandable to four (4)

UNIX-based systems such as machines from SUN and Hewlett Packard (HP) were also evaluated. With the workload of less than 20 requests per day and estimated growth over the next three years to be less than 50 concurrent users, the selected "SMP" Pentium Pro offered a far superior cost benefit ratio.

Operating System

Windows NT Server 4.0

Software

RDBMS: Oracle 7.3

Web Server: Oracle Web Server 3.0

Middleware: EDA/SQL server

If the workload exceeds the predicted value in the future, this configuration provides a great deal of expandability. First, two (2) more CPUs can be added without affecting any existing software or hardware component. Second, the RDBMS can be moved to a separate system to provide further expandability.

4.5.3.2 Client-Contractors, Government Agencies, and Department Control Points

Clients are those who submit DD Form 61 requests to the TDAS. There are four types of clients: Department Control Points, Government Agencies, and contractors². In this CONOPs and the initial development of the TDAS for CECOM, the focus is on contractors and Department Control Points. The Government Agency ability is identical to the Department Control Points and functions only as an additional level of approval in the four tier architecture. Any reference to Department Control Point herein after will infer Government Agency with respect to functionality. A contractor is an organization that is developing or modifying a system or part to be nomenclatured. They fill out the information about the item on the DD Form 61 and wait for the pre-approval from the Department Control Point before being processed by CECOM or AFMC. Special attention is paid to the recommended item name, type designation, and source request number. The Department Control Point will then submit the DD Form 61(s) to the DoD Control Points for final approval. The Department Control Point is the middle layer between the contractor and the DoD Control Point.

The only external hardware and software requirements to these clients (contractors, Government Agencies, and Department Control Points) who submit DD Form 61(s) electrically and perform simple data inquiry is a Web browser such as Netscape Navigator or Microsoft Explorer and Internet access. Because the Web application resides on the TDAS server itself, there is no software updating cost associated with each client. The client may need to download a plug-in (one-time occurrence) through the Web browser to initially execute the TDAS application residing on the server. The client also may need to perform a one-time download of SQLNET. Both of these downloads along with instructions will be provided on the TDAS Web page. Modification to the application will not have any effect on the clients except possible change of the interface.

<p>Clients who spend extensive time using TDAS may be provided with the TDAS stand-alone version of the software. Performance would be slightly better; however, configuration management of the software would need to be maintained. Access by these clients would be determined by the DoD Control Point.</p>
--

4.5.3.3 DoD Control Point

A DoD Control Point has a differing role from the other users mentioned earlier. A DoD Control Point performs data inquiry and needs to be able to edit/correct the data, approve DD Form 61 requests, and generate reports. Consequently, the DoD Control Point application will be more complicated than client Web application. PowerBuilder from Powersoft has been identified as the development tool for the DoD Control Point application. Two of the major advantages of PowerBuilder are its object-oriented Rapid Application Development (RAD) and scaleable capabilities. Because PowerBuilder is easy to learn, developers will be able to modify the TDAS application in the future if they choose to do so.

The connection to the Oracle database will utilize the existing LAN infrastructure. Although a DoD Control Point needs more functionality than a client does, a typical Intel-based system will be enough for its tasks. The DoD Control Point configurations will consist of:

- (2) CompuNet Nspire Pentium Pro Workstations
- 200 MHz
- 64 MB memory
- 4.3 GB hard drive
- Microsoft Office 97

4.5.3.4 Telecommunication

Because Oracle and EDA/SQL are both capable of supporting multiple network protocols, there is no need to alter the current LAN infrastructure to accommodate TDAS. The Web approach does require the external clients to have access to TCP/IP.

Because TCP/IP is the most widely used protocol today, it can be easily acquired, either through a direct LAN/Wide Area Network (WAN) connection, or through a dial-up connection from Government-supported agencies or commercial Internet Service Providers (ISPs).

5.0 OPERATIONAL SCENARIOS

This section highlights several typical operations that will be performed by the contractor, Department Control Point, and DoD Control Point. These operations only serve as examples of how users will interact with the TDAS and how they will be benefited from the TDAS.

Table 5.0-1 shows the proposed TDAS actions available to the various user groups. Further detail is to follow throughout this section.

Table 5.0-1 TDAS Action Command Matrix for Various Users

Users Actions	DoD Control Point	Department Control Point	Government Agency	Manufacturing Contractor	Administrative Contractor
Process Package	✓	✓	✓		
Process Submittal	✓	✓	✓		
Prepare New Package	✓	✓	✓	✓	
Prepare New Form	✓	✓	✓	✓	
Modify a Rejected/ Unfinished Form	✓	✓	✓	✓	
View Form	✓	✓	✓	✓	✓
Reserve Nomenclature	✓				
Add Paper Form (Legacy)	✓				
Associate Images with Form	✓				
Delete Form From Database	✓				
Notify Originator of Completed Form/Package		✓	✓		

5.1 TDAS Client View (Contractors and Department Control Point/Government Agency)

There are two categories (4 total users types) of external clients:

1. Contractors, which refers to either a Manufacturing Contractor that initially fills out and submits the DD Form 61(s) for pre-approval, or Administrative Contractors that can only browse through approved DD Form 61 information.
2. Department Control Points/Government Agencies have the responsibility for pre-approving that the information filled out is complete and correct before being processed by CECOM or AFMC DoD Control Point.

All of these activities will be done from a Web browser accessing TDAS's Uniform Resource Locator (URL).

5.1.1 Submittal of DD Form 61(s)

The following is a typical scenario showing how Manufacturing Contractors can submit DD Form 61(s):

1. Access TDAS's URL from a Web browser, provided TCP/IP has been acquired either through a direct or dial-up connection.

2. Fill out the form from the browser, as the user would normally do on the paper. This form resembles the look and feel of current DD Form 61(s) with only minor modifications in order to comply with HyperText Markup Language (HTML) syntax and format. Because of the resemblance between the Web form and the paper DD Form 61, users will be able to adjust to the Web interface easily.
3. Submit the form by clicking on the “submit” button. Intelligence will be built into the Web application to validate the inputs for some formatting and required entries. It will then inform the users about the errors, thus shortening the turn around time and alleviating some of the burden from the Department Control Point personnel.
4. In order to denote which Department Control Point should receive the DD Form 61(s), a special control sequence will be attached to this DD Form 61 request. It will either be filled out by the contractor or derived automatically from the username and password if applicable. The control sequence is to be used as an identifier that will allow only the appropriate Department Control Point to have access to this DD Form 61 for the pre-approval process. In other words, the control sequence is a link between a contractor and his/her Department Control Point.
5. Finally, the DD Form 61 request just being submitted will have the status of “waiting-for-pre-approval.” There will be a built-in notification mechanism in the TDAS to inform the appropriate Department Control Point, indicating that there is a request waiting for the pre-approval.

When a user wants to submit a package of related DD Form 61s, they can proceed as described above because the “package” will be handled by the modified SRN that is agreed on by CECOM. The modified SRN will clearly indicate the total number of related DD Form 61s that have been submitted and the order of each DD Form 61 in this package.

5.1.2 Manufacturing Contractor Functional Description

A Manufacturing Contractor is responsible for preparing and submitting a new item or system that is being processed for type designation and nomenclature. Manufacturing Contractors fill out DD Form 61(s) and submit them to Department Control Points. The Manufacturing Contractor will use TDAS to create a new DD Form 61 in order to begin the process of acquiring a type designation for a new piece of equipment. Manufacturing Contractors then submit the completed DD Form 61, or a package comprising several DD Form 61(s), to a Department Control Point. This type of contractor has submittal privileges, as well as viewing privileges for data that they have submitted. The primary procedures performed by a Manufacturing Contractor using TDAS include the following:

I. Request Login and Password.

II. Enter TDAS.

1. Access TDAS via the Web.
2. Input Login and Password.
3. Receive Initial Screen. (This initial screen should have any alerts, notices, and completions for this contractor displayed.)

III. Choose Type of Action.

1. Prepare a package. A package is a set of related DD Form 61s that will be submitted together for type designation and nomenclature reservation. Manufacturing Contractors should not input an unrelated DD Form 61 as part of a package, because if the unrelated DD Form 61 is rejected, the entire package will be rejected. Instead, the Manufacturing Contractor should submit the unrelated DD Form 61 separately.
2. Prepare a single assignment request.
3. Request revision to a single existing type designation.
4. Request a cancellation to a single existing type designation.
5. Modify and resubmit a rejected submittal.
6. Retrieve a DD Form 61.
7. View all submittals (only for contractor-originated submittals).
8. View pending submittals (only for contractor-originated submittals).
9. View approved submittals (only for contractor-originated submittals).
10. View rejected submittals (only for contractor-originated submittals).

See Appendix D, Functional Flows for more details on these functional flows.

5.1.3 Administrative Contractor Functional Description

An Administrative Contractor gathers information from the TDAS (through “read-only” access) for Government agencies. Administrative Contractors are not permitted to create, modify, or delete any information within TDAS. Administrative Contractors cannot see any other than completed, approved DD Form 61s. The primary procedures performed by an Administrative Contractor using TDAS include the following:

I. Request Login and Password.

II. Enter TDAS.

1. Access TDAS via the Web.
2. Input Login and Password.
3. Receive Initial Screen.

III. Choose Type of Action.

1. Retrieve a DD Form 61 for viewing.
2. View all submittals.
3. View pending submittals.
4. View approved submittals.
5. Request a report.

See Appendix D, Functional Flows for more details on these functional flows.

5.1.4 Department Control Points/Government Agency Pre-approval of DD Form 61

A Department Control Point and/or Government Agencies (also called a “pre-approval point,” a “program office,” or a “program manager”) has the responsibility for pre-approving the correctness and completeness of information in the DD Form 61(s) that they receive from Manufacturing Contractors. They are the official control points within the military departments authorized to obtain joint electronic type designations from the DoD control point or appropriate branch. Department Control Points use the TDAS system to pre-approve or reject a type-designation action received from a Manufacturing Contractor in CECOM case.

The following scenario typifies how a Department Control Point would pre-approve DD Form 61 requests in the new system:

1. Access TDAS’s URL from a Web browser, provided TCP/IP has been acquired either through a direct or dial-up connection. Because of the control sequence, a Department Control Point will be allowed to access only those requests under its control.
2. Verify that the information on the DD Form 61 is correct and complete and assign the SRN.
3. Submit the form by clicking on the “pre-approve” button. Similarly, intelligence will be built into the Web application to validate the inputs for some formatting and required entries. It will then inform the users about the errors, thus shortening the turn around time and alleviating some of the burden from TDAS personnel.
4. Finally, the DD Form 61 request just being pre-approved will have the status of “pre-approved.” Also, there will be a built-in notification mechanism in the TDAS to inform the CECOM or AFMC that there is a request waiting for the approval.

When an error is found, the Department Control Point can either correct the error (if that is allowed), contact the submitter for further action, or open a window in TDAS to summarize the problem. The submitted DD Form 61 with the problem annotation can then be sent back to the submitter for reworking.

5.1.5 Department Control Point/Government Agency Functional Description

The Department Control Point described in Section 5.1.4, carries out his tasks according to the following functional workflow.

- I. Request Login and Password.
- II. Enter TDAS.
 1. Access TDAS via the Web.
 2. Input Login and Password.

3. Receive Initial Screen. (This initial screen should have any alerts, notices, and completions for this contractor displayed.)

III. Choose Type of Action.

1. Prepare a package. A package is a set of related DD Form 61(s) that will be submitted together for type designation and nomenclature reservation. Department Control Points should not input an unrelated DD Form 61 as part of a package, because if the unrelated DD Form 61 is rejected, the entire package will be rejected. Instead, the Department Control Point should submit the unrelated DD Form 61 separately.
2. Prepare a single assignment request.
3. Request revision to a single existing type designation.
4. Request a cancellation to a single existing type designation.
5. Modify a rejected submittal.
6. Retrieve DD Form 61.
7. Process a submittal.
8. Process a package.
9. Notify originator of completed form or package.
10. View all submittals.
11. View pending submittals.
12. View approved submittals.
13. View rejected submittals.

See Appendix D, Functional Flows for more detail on these functional flows.

5.1.6 Data Inquiry for Clients

TDAS clients, both contractors and Department Control Points, will be given the ability to perform specific data inquiries into the TDAS system database. The viewing (read) privileges are to be determined by their respect access levels granted through the DoD Control Point (CECOM/AFMC) administration. The capability to submit pre-determined queries will be included in the TDAS system. For example, the user could query using a part number or drawing number or could query about a particular DD Form 61 request to see if it has been processed and the status of the form. Other structured queries will be built into the application for clients to perform. For example, if the user queries upon a particular source request number, part number, or drawing number, the query will be sent to the database. Results from the query will then be compiled and presented to the user in a single and uniform view.

5.2 TDAS DoD Control Point View

The DoD control point, as a DoD Control Point, is officially responsible for the assignment of type designations. DoD Control Points constitute the official DoD assigning agency responsible for assigning type designations within the TDAS at CECOM. DoD Control Points are responsible for approving, rejecting, or revising DD Form 61 requests, generating various reports, and performing other tasks to support their day-to-day duties. Therefore, they will be given the highest level of access privileges to the database system, which includes full read, full write, and full delete privileges. The DoD Control Point receives the completed, pre-approved

DD Form 61(s) from the Department Control Points and uses TDAS to assign to each type a unique designation.

5.2.1 Approval and Update of DD Form 61(s)

The “package concept,” which refers to a group of DD61(s) for a particular configuration item/system that consists of the related sub items/systems being processed for type designation and nomenclature, is important in the approval process. It is more reasonable to process each package all together than to jump from one request in one package to another request in another package. The TDAS will facilitate this “package concept” by allowing approval only when an entire package of DD Form 61(s) has been received.

The default processing order of the approval will be first come, first serve. However, from the DoD Control Point application, a user will be given the capability to select which pending DD Form 61 requests to process. For example, a DoD Control Point can select and process the DD Form 61 requests from the same originator or with a related type designator in a group - whichever makes sense for a particular circumstance.

The pre-approved request will be shown on a DoD Control Point screen with the same look and feel of the existing paper DD Form 61. In a manner similar to the client Web-based application, validation rules will be built into the application to assist the DoD Control Point in the approval process. With full access to the database, the validation rules can be very comprehensive. For example, a request for revision can be approved only if there is an assignment for the same nomenclature.

When an error is found, the DoD Control Point can correct the error (if that is allowed), contact the submitter for further action, or open a window in TDAS to summarize the problem. The submitted DD Form 61 with the problem annotation can then be sent back to the Department Control Point for reworking. Once a request has been validated by both the TDAS personnel and the application, an E-Mail message, or other communication mechanism will notify the submitter that the request has been approved. The submitter will also be notified of any modification that has been made to the request. Finally, the approved DD Form 61 will have the status “approved” and be stored permanently in the TDAS for future references.

5.2.2 DoD Control Point Functional Description

The DoD Control Point, described in Section 5.2, carries out his tasks according to the following functional work flow:

- I. Request Login and Password.
- II. Enter TDAS.
 1. Access TDAS via the Web.
 2. Input Login and Password.
 3. Receive Initial Screen. (This initial screen should have any alerts, notices, and completions for this contractor displayed.)

III. Choose Type of Action.

1. Prepare a package. A package is a set of related DD Form 61(s) that will be submitted together for type designation and nomenclature reservation. DoD Control Points should not input an unrelated DD Form 61 as part of a package, because if the unrelated DD Form 61 is rejected, the entire package will be rejected. Instead, the DoD Control Point should submit the unrelated DD Form 61 separately.
2. Prepare a single assignment request.
3. Request revision to a single existing type designation.
4. Request a cancellation to a single existing type designation.
5. Modify a rejected submittal.
6. Retrieve DD Form 61.
7. Process a submittal.
8. Process a package.
9. Reserve nomenclature.
10. Delete DD Form 61 from database.
11. View all submittals.
12. View pending submittals.
13. View approved submittals.

See Appendix D, Functional Flows for more detail on these functional flows.

5.2.3 Data Inquiry

The data inquiry activity will be very similar to the one described in the client section, except this is done from the PowerBuilder application with more complicated query capability. Some standard queries will be built into the DoD Control Point application, but they can also be customized easily for each TDAS. Reference Section 5.2.5 Report Generation. The LAN/WAN network connectivity of the DoD Control Point to the server will allow for greater performance and response time from the database server.

Additional query capability would be available to the DoD Control Point via standard Oracle SQL tools.

5.2.4 Tracking

All the tracking data will be logged into the database automatically by the DoD Control Point application. Review of the tracking data will be available through the Report Generation functionality. (See Section 5.2.5). Information may include, but is not limited to the following:

- When a DD Form 61 request is submitted.
- When a request is processed.
- When and why the approval process is on hold.
- When and why a request is rejected.
- When a request is approved.

This information will provide a detailed history of each DD Form 61 request. It not only can be utilized to provide better contractor service, but it can also serve an internal-monitoring purpose.

5.2.5 Report Generation

The TDAS will have the capability to do custom reports. Common reports will be included in the DoD Control Point application, as well as being accessible to the appropriate clients. Most importantly, the reporting capability can be fully customized by each MSTDS to meet its own mission. For example, a TDAS could generate a summary report of DD Form 61 requests submitted by a particular originator within a certain period of time or a performance analysis report indicating average turn-around time from submittal to approval. Table 5.2.4-1 shows the proposed TDAS Report for the various users.

Table 5.2.4-1 TDAS Report Command Matrix for Various Users

Actions:	Users:	DoD Control Point	Department Control Point	Government Agency	Manufacturing Contractor	Administrative Contractor
View All Submittals		✓	✓	✓	✓	✓
View Pending Submittals		✓	✓	✓	✓	✓
View Approved Submittals		✓	✓	✓	✓	✓
View Rejected Submittals		✓	✓	✓	✓	✓
Close Out Non-Army DD Form 61s		✓				
Close Out Army DD Form 61s		✓				
Statistics Overall		✓	✓	✓		
Statistics by Technician		✓	✓	✓		
Statistics by Proponent		✓	✓	✓		
Statistics by Proponent and Action		✓	✓	✓		
Duplicate Design Parts		✓	✓	✓		
Duplicate Manufacturing Parts		✓	✓	✓		
Duplicate Contractor Parts		✓	✓	✓		

6.0 ANALYSIS OF THE SYSTEM

The advantages of the TDAS are summarized in this section. Some alternatives and trade-offs considered during the design phase are also discussed.

6.1 Summary of Advantages

Following are the major advantages provided by the TDAS. These advantages are provided either by the approach taken to implement the TDAS, the design of the database, or simply the automation of the MSTDS.

Automation of MSTDS

- Reduction of turn-around time from submittal to approval or rejection.
- Elimination of the error-prone ledger books.
- Full and easy access to the history of each DD Form 61.
- Reduction of manpower and human mistakes with built-in verification and validation.
- Capability of generating various reports.
- Capability of online data inquiry.

Client/Server Computing

- Better leveraging of emerging desktop computing technology.
- Reduction in network traffic.
- Encouragement of an open system with the flexibility of the selections of both front-end development and back-end database server.
- Ease of training and user acceptance by using a GUI.
- Performance and scalability in improving query performance against large tables.
- Integrity and security because of the separation of client application and the data.

WWW/Internet

- Reduction of software distribution, installation, and updating costs.
- Reduction of support and maintenance costs.
- Greater acceptance by users since there is no application to be installed to their systems.

Reduction of training costs through the usage of a common and user-friendly Web browser interface.

Ease of access to the TDAS since no additional hardware or software purchase is required except TCP/IP and a Web browser.

Enhanced reliability because of the Internet's designed-in graceful degradation.

6.2 Alternatives and Trade-offs Considered

Several alternatives considered during the design of the TDAS are described in this section.

6.2.1 TDAS Server Hardware

The selection of TDAS server hardware is primarily based on the following three criteria: performance, cost (including both purchasing and maintenance/service costs), and computing power required of the TDAS. Systems considered included SUN and HP running UNIX operating system, and Intel Pentium Pro running Microsoft Windows NT. Although mid-range to high-end systems from SUN and HP provide greater performance, they were determined to be both too costly and unnecessary, from a price/performance perspective, for a TDAS server. In addition, a low-end SUN or HP does not perform as well as a Pentium Pro system with the same price.

6.2.2 Web Application Development

Many development approaches have been considered: Fourth-Generation Language (4GL) client/server development tools with extensions for the Web, such as PowerBuilder; the Java development tool with Java Database Connectivity (JDBC); Web application server tools including Oracle Web Server and ColdFusion. The selection of the tool, like the selection of the TDAS server hardware, was constrained by budgetary, time, and performance constraints. Therefore, some of the tools that posted the highest technical merits were not evaluated because of their high costs and development time.

A Java approach provides a high-degree of platform support and richer programming features but its immaturity is a major concern. The Web-application server approach does not require other client software. This makes the approach more suitable for the TDAS application. Furthermore, Oracle Web Server is designed mainly for the Oracle RDBMS, and thus, has the advantages of better performance and security among all the alternatives. However, both the Oracle Web Server and ColdFusion use an HTML-like programming toolkit. Since HTML is not a programming language, this essentially limits the programmer's ability and creativity within the Web interface design.

7.0 TDAS IMPLEMENTATION ISSUES

Key implementation issues are addressed in this section, including legacy data conversion, EDA/SQL software, security concerns, database schema design, and performance.

7.1 Legacy Data

Type-designation data has been stored in many different media. These include:

- The original paper DD Form 61(s).
- Images of DD Form 61(s) on Canonfile optical disks.
- Microfilm.
- Microfiche.
- UNISYS 9 track tape in S2K format.
- The tracking databases that have a subset of the data.
- Ledger books that contain a subset of the data.

This scenario creates a number of issues. Obviously, the first issue is that data will have to be converted from various formats into American Standard Code for Information Interchange (ASCII) format, which can then be entered into the TDAS database. We originally believed that it was only necessary to use three media - paper, microfiche, and S2K - to cover all data from 1943 to the present. However, this still presents challenges in using different equipment and conversion processes to convert each medium. The present plan is to use a conversion service to convert paper and microfiche data. The S2K format presents a special challenge that is discussed below.

Another issue is that microfiche is not in the DD Form 61 format. In fact, the microfiche, which appears to cover the years 1943 to 1969, contains images of at least four different forms. These forms do not include some DD Form 61 fields. In addition, some data elements that are equivalent to DD Form 61 data elements in meaning are named differently on the microfiche forms than those DD Form 61 elements. Thus, any attempt to automate conversion would mean that separate scripts would have to be developed for each medium, and the database schema would have to be more complex in order to accommodate all of the data fields.

We are unsure of the S2K format as CECOM, as well as this task, has pursued many avenues to read UNISYS 9 track tapes but has been unable to do so, as the S2K format is obsolete. This inability to read S2K data at this time is a third issue. The S2K data covers the years from 1970 to 1986 and, being in a database format already would seemingly provide the least conversion challenge. However, we have not been provided with a data dictionary for this database, and we have not seen one single record, so we have no way of knowing how closely this format matches the DD Form 61 format. It is likely that a third script would need to be developed for this medium and it is possible, if more or different fields are discovered, that the database schema will be further complicated. Due to the problems with reading S2K, we have decided to use backup microfiche data for the years 1970 to 1986.

There are large amounts of data in each medium. Our current estimates are 82,500 pages of paper, 176,000 pages of microfiche from 1943 to 1969, and 75,000 records on microfiche from 1970 to 1986. Data conversion is labor intensive and there is very little volume discount.

There are visual aspects of some of the data, at least of paper and microfiche, that will cause errors or be unreadable by automated conversion or human data entry. These aspects include handwriting, illegible data entries, multiple fonts, degradation of data due to xerographic copying, and data in technical data block 14 not following the prescribed format. Close investigations of 111 paper forms shows that every one has some handwriting and up to 23% have some visual aspect that will cause conversion problems. Thus, each page will need human inspection after conversion, raising the cost. In addition, some entries (poor handwriting, illegible) will require CECOM expertise to ensure that the correct data is entered.

The diversity of format-and-medium combinations with the visual aspects of some data forms, mean that automated data-conversion, followed by use of single or multiple scripts to automate the database-entry process, is not feasible without substantial human inspection. This method would produce only a 90-93% data replication. Therefore, we have decided to use manual keystroke entry combined with scanning of each DD61 or microfiche image. The cost of such an alternative is based on the number of keystrokes. In order to reduce this cost to an acceptable level, only the essential fields will be keyed in. The associated images will be stored in the database.

In this procedure, each page of the DD Form 61(s) is scanned to produce a TIFF 4 image. Key fields for each image are entered by hand into a database linked to the images. The output of the conversion process will need to be inspected by the service provider. They can provide correction and flag problems that need expert (i.e., CECOM) attention, such as deciding what should be entered when the handwriting or the typewritten entry is barely legible. CECOM experts will then have to work on those pages to enter the correct data. CECOM will also have to do random checking of all converted data to verify the data. After loading into a database via scripts, CECOM experts will have to randomly check and verify that the script has functioned correctly. In this way, we can reach a high degree of quality (approaching 99%) of replication of the important legacy data - a degree of quality unattainable with automated methods at this time.

Due to time and cost considerations, it has been decided, with CECOM concurrence, to convert only data from 1970 to the present.

7.2 The DLSC Information Hub

The lack of MSTDS connectivity contributes to the duplication of acquisition and logistics efforts, the inability to find parts in inventories, the duplication of parts in inventories, and numerous other logistics-management issues. The DLSC information hub will allow for access to parts information in the FLIS and MSTDSs through a single user-interface. This system will allow a user to enter certain key information (e.g., a part number or type designation) and discover which systems had information on a part and what the information is.

The DLSC information hub is to provide a single entry point and a single online query session with the ability to cross-reference multiple TDASs and the FLIS. Although the objective of the DLSC information hub is both well defined and achievable, the use of EDA/SQL to facilitate an integrated, query capability across the various MSTDSs remains a prevailing concern. Using the proposed architecture, EDA/SQL is required at both the CECOM TDAS and the DLSC information hub locations in order for information to be exchanged among the two. With this architecture, TDAS users outside of the CECOM LAN cannot query from the DLSC information hub. We recognize this as an existing limitation and are planning to propose a solution that will enable access to the DLSC information hub from a Web browser via the TDAS at CECOM.

7.3 EDA/SQL

The deployment of EDA/SQL server software is required by DLSC. The EDA/SQL provides the capability of accessing multiple data sources, including relational databases and mainframe non-relational databases, and presents the result back to users in a uniform manner. However, because of its proprietary nature, the only way to communicate with EDA/SQL software is from another EDA/SQL software package. Furthermore, the EDA/SQL client software is very expensive, from not only a purchasing standpoint but also because of the high levels of maintenance effort and costs. Training or service support will be necessary for each TDAS because of the complexity of EDA/SQL software. Another major disadvantage is the implementation of the catalogue server module which stores the information of other catalogue servers for the naming translation among various data sources. Any change to one TDAS database schema, as long as the change is in the public interest, will necessitate an update to all the other catalogue servers, because there is no automated updating capability within the EDA/SQL software. All updating will need to be carried out manually. This burden will grow as the number of TDAS installations increase.

7.4 Security

Security is a baseline requirement for network computing that includes both client/server and WWW/Internet approaches in our design. Privacy, authentication, authorization, and data integrity are important elements of any security strategy. These practices work to defend against the threats of eavesdropping, manipulation, and impersonation. The purpose of this section is to discuss security features that will be implemented in the TDAS and other security measure that might be of interest to each MSTDS. It is not our intent to influence any current security practice at each MSTDS, nor do we suggest that one measure is better than another is. Security information will be provided to each MSTDS, as requested.

7.4.1 User Authentication

User authentication can be detailed in two categories for the TDAS clients. Both stand-alone and Web based environment approaches are discussed in the following sections.

7.4.1.1 Stand-alone Application in a Network Environment

Accurate identification is a prerequisite for security. The correct username and password are required in order for a DoD Control Point or client to access the TDAS. Each external client will need to apply a valid username and password before accessing TDAS Web pages. Thus, each TDAS will have full control of who will be granted the access privilege. Naming conventions and other rules on assigning a username and password will be totally up to each TDAS. However, it is common for users to write down their passwords in exposed places or to divulge them to others. Therefore, it is recommended that passwords should be changed periodically.

7.4.1.2 World Wide Web Based Application in a Network Environment

There are currently three methods for authenticating users of Web browsers: (1) basic authentication, (2) digest authentication, and (3) "digital identification" (using digital signatures and certificates). Basic authentication is the current standard for Web authentication and is specified in the HTTP/1.0 specification, the current protocol underlying the WWW. Both Microsoft and Netscape support this level of authentication with the 3.x and later versions of their Web browsers. This method provides a very weak authentication since both user identifier and password are encoded in Multi-purpose Internet Mail Extensions (MIME) base64 type, which is unencrypted. Therefore, this method of authentication is susceptible to threats like packet sniffers that may intercept the user identifier and password and use a shareware product like Winced to decode the base64 message into clear text.

Digest authentication, proposed as part of the new HTTP/1.1 specification, provides a somewhat safer authentication level since the user identifier and the password will be encrypted (see Internet Request for Comments 2068 and 2069¹) using a message digest technique that employs a one-way hashing algorithm to encrypt an arbitrary length message into an encrypted 128-bit or 160 bit digest. Current Netscape and Microsoft Web browsers (versions 4.x) do not support this proposed standard. A third level of authentication uses digital signatures (and digital certificates) and encryption. The digital signature is an encoded bit stream of information in a message or transmission that identifies the user of a Web browser or the sender of an E-Mail message, or the author of a software component like an ActiveX control or Java applet. A Digital Signature Standard (DSS) has been adopted by the National Institute of Standards and Technology (NIST) and published as a Federal Information Processing Standard (FIPS) Publication 186, but this standard has not gained wide commercial support. Digital signatures based on public key cryptography have been incorporated into other proposed standards documents, notably S/MIME for electronic mail,² and MIME-based Secure- Electronic Data Interchange (EDI) for EDI over the Internet.³ These methods generally permit a variety of encryption algorithms; thus, one need not be locked into a proprietary algorithm (e.g., RSA) or an algorithm that has received substantial criticism (e.g., NIST's DSS). The WWW Consortium (W3C) is also working on a

¹ RFC 2068 -HyperText Transfer Protocol -- HTTP/1.1. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, T. Berners-Lee. January 1997, and RFC 2069, An Extension to HTTP: Digest Access Authentication. J. Franks, P. Hallam-Baker, J. Hostetler, P. Leach, A. Luotonen, E. Sink, and L. Stewart. January 1997. <http://www.internic.net/ds/rfc-index.2000-2099.html>

² S/MIME Message Specification, Nov 8, 1997. <http://ds.internic.net/internet-drafts/draft-dusse-smime-msg-06.txt>

³ MIME-based Secure EDI, Internet Draft, draft-ietf-ediint-as1-03.txt; Mats Jansson, LiNK; Chuck Shih, Actra; Nancy Turaj, Mitre Corp.; and Rik Drummond, Drummond Group. 10 January 1997. Source: <http://www.commerce.net/services/portfolios/edi/pilot/draft-ietf-ediint-as1-03.txt>

digital signature standard as part of its Digital Signature Architecture Initiative.⁴ Although there is not yet a universal standard for digital signatures, both Netscape and Microsoft support digital signatures and encryption in the latest versions of their browsers (version 4.x).

Recommendations: At a minimum, adopt digest authentication when Commercial Off-The-Shelf (COTS) products are available to support this method. If stronger user-authentication is required, adopt products that support digital signatures and encryption. Assess the administrative workload impact of adopting and implementing digital signatures and digital certificates.

7.4.2 Database-Level Security

In addition to basic user-authentication, database-level of security will be implemented. As mentioned, the external client can only perform submitted and query functions against the TDAS database. In addition, a submitted DD Form 61 request will need to be approved by a DoD Control Point before it can be permanently stored in the database. With these implementations, an unauthorized external access resulting from a stolen password and even an intentional misuse of the system will not damage the integrity of the database.

7.4.3 Internet Security

Security on the Internet is a complex subject. Although there are many potential weaknesses and many diverse types of attacks, one should not be discouraged by the usage of Internet computing. With appropriate measures, Internet computing can be safe and efficient. The following paragraphs are brief discussions of some of today's popular security technologies, which might be of interest to each TDAS. We address each technology in five areas:

1. The problem that the technology solves.
2. Description of the technology.
3. The level at which the technology may be implemented.
4. The types of platforms on which the technology has been implemented.
5. The efforts to obtain consensus and standardization.

7.4.3.1 Virus Detection, Identification, and Eradication

The Internet has introduced a new source of virus exposure with both the downloading of information and E-Mail attachments from anywhere in the world. Macro viruses incorporated in Word files and corporate-groupware solutions are now sources of infection that spread rapidly through an enterprise. The sharing of diskettes is also a common way for a virus to spread. A multi-layered defense strategy that includes desktop, server, groupware, and Internet gateway-based solutions for total virus protection, is needed. Anti-virus technologies include software virus detectors, identifiers, and removers.

Security Problem That Is Addressed:

Denial of service.

⁴ Proposed Digital Signature Architecture Initiative. <http://www.w3.org/TR/WD-DSIG-arch.html>

Technology Implementation Level (application, presentation, session, transport, network, link):
Application Gateway, file server.

Platforms Support:

UNIX, Windows NT, Windows 95. Vendors include McAfee, Symantec, Cheyenne, Trend, and Soloman. McAfee leads this market with a dominant a 52% market share.

Industry Adoption/Standardization:

There are no industry standards. McAfee leads market with a 52% share.

Recommendations:

Purchase NetShield Virus Detection, Identification, and Eradication software for Windows NT 4.0 servers.

7.4.3.2 Firewalls

Firewalls are software and/or hardware products that precisely define, control, and limit access to internal computers from outside computers across a network. Firewalls are most often employed to limit exposure when connecting an organization's network to the Internet or other external or untrusted networks. Firewalls are also used to deter hackers and other unauthorized users from damaging or obtaining unauthorized access to, internal computers, data, and computing resources.

Security Problem That Is Addressed:

Access control.

Technology Implementation Level (application, presentation, session, transport, network, link):
Four schemes are referred to as "Firewalls."

1. Application Level Gateways.
2. Proxy Servers (Circuit Level Gateways).
3. Packet Filters.
4. Stateful Packet Inspection (Dynamic Firewall Technology).⁵

Each of these perform different functions and operate at different levels in the Open System Interconnect (OSI) 7 layer model: 1) session levels (e.g., packet filters), and 2) application level (e.g., for bastion hosts).

Platforms Support:

UNIX, Windows NT servers; multiple vendor products

Industry Adoption/Standardization:

National Computer Security Association (NCSA) has a firewall certification process for certifying firewall products.

⁵ Ascend Firewall 101: Internet URL: <http://www.ascend.com/861.html>

7.4.3.3 SOCK Network

SOCKS is a proxy system equipped with security, auditing, management, fault tolerance, and alarm notification. The most traditional and common use for SOCKS is as a network firewall, even though SOCKS is much more than just a firewall. SOCKS is networking Middleware that enables an unstructured, and often unsecured enterprise network, to effectively, responsibly, and safely use the Internet. SOCKS establishes a secure proxy data channel between two computers in a client/server environment. From the client's perspective, SOCKS is transparent. From the server's perspective, SOCKS is a client.⁶

Security Problem That Is Addressed:

Access Control (SOCKS V4) and authentication (SOCKS V5)

Technology Implementation Level (application, presentation, session, transport, network, and link):

Application level

Platform Support:

UNIX and Windows NT servers

Industry Adoption/Standardization:

Internet Engineering Task Force (IETF) Request for Comments (RFC)1928 - Describes SOCKS Version 5 protocol, also known as Authenticated Firewall Traversal (AFT);⁷ IETF RFC 1929, Username/Password Authentication for SOCKS V5;⁸ and IETF RFC 1961 - Describes Generic Security Service (GSS)-Application Programming Interface (API) authentication for SOCKS V5.

7.4.3.4 Public Key Cryptography (PKC)

Public key technology involves the use of a pair of related keys, one of them is freely distributed and another that is tightly controlled by the owner. These keys are algorithmically related such that a message encrypted by user A with the public key of user B can only be decrypted by user B, even though the encryption key used by user A is known to all. Furthermore, public keys have the property that if a message is encrypted with user A's secret key, then user B, in possession of user A's freely distributed public key, can decrypt the "signature" and authenticate that only user A could have originated the message. The obvious benefit of the technology is that clients and servers could use public known keys and encrypt messages or decrypt signatures to protect and validate transactions. There is no need to distribute a key, a problem with traditional encryption implementations like the Data Encryption Standard (DES). There is, however, a major problem with dissemination of public keys. Although one part of the key is public, there is nothing inherent in the model to prevent user C from placing a public key in the public domain and claiming it to be user A's public key. The solution to this problem is the use of commercial third party certification authorities that issue certificates to users.

⁶ Introduction to SOCKS, <http://www.socks.nec.com/introduction.html>

⁷ SOCKS FAQ , Internet URL: <http://www.socks.nec.com/socksfaq.html#q12>

⁸ [http://www.globecom.net/\(nobj,sv\)/ietf/rfc/rfc1929.shtml](http://www.globecom.net/(nobj,sv)/ietf/rfc/rfc1929.shtml)

Security Problem That Is Addressed:

User authentication, message integrity.

Technology Implementation Level (application, presentation, session, transport, network, link)

Applications level:

Multiple products have been developed using the RSA cryptography toolkits. Categories include developer's toolkits, electronic commerce and EDI, E-Mail, groupware, forms and workflow, firewalls, remote-access, general security utilities, Internet browsers and servers, notarization and ID systems, operating systems, smart cards and tokens, storage management and content distribution, telephony, modems and facsimiles, and wireless communications.⁹

Platform Support:

UNIX, Windows 95, and NT.

Industry Adoption/Standardization:

RSA Public Key Cryptography Standards (PKCS): The informal inter-vendor standards were developed in 1991 by RSA Laboratories with representatives of Apple, Digital, Lotus, Microsoft, MIT, Northern Telecom, Novell, and Sun. Since its publication in June 1991, PKCS has become a part of several standards and products, including Internet Privacy-Enhanced Mail, NIST/OSI Implementers' Workshop, BLOC F3 Forms Automation, Apple's PowerTalk, Shana Informed, and Fischer International's Workflow 2000.¹⁰

7.4.3.5 Secure Socket Layer

Netscape has designed and specified a protocol for providing data security layered between application protocols such as HyperText Transfer Protocol (HTTP), Telnet, Network News Transfer Protocol (NNTP), or File Transfer Protocol (FTP) and TCP/IP. This security protocol, Secure Socket Layer (SSL) provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. A variety of cryptographic algorithms is supported by SSL. During the "handshaking" process, the RSA public-key cryptosystem is used. After the exchange of keys, a number of ciphers are used. These include RC2, RC4, IDEA, DES, and triple-DES. The MD5 message-digest algorithm is also used. The public-key certificates follow the X.509 syntax.¹¹ It is important to track emerging developments with this protocol due to the rise in popularity of the Netscape browser and its influence on the Web community.

Security Problem That Is Addressed:

Web transaction (Message integrity) and server and client authentication.¹²

Technology Implementation Level (application, presentation, session, transport, network, link)

Transport:

⁹ RSA Security Solutions Catalog: http://www.rsa.com/rsa/PRODUCTS/sscat_winter96/97wor/index.html

¹⁰ RSA Laboratories PKCS: <http://www.rsa.com/rsalabs/pubs/PKCS/>

¹¹ RSA Labs Security FAQ: <http://www.rsa.com/rsalabs/newfaq/q134.html>

¹² SSL Reference Document, Netscape Communications: <http://home.netscape.com/info/security-doc.html>

The SSL protocol is application independent, allowing protocols like HTTP, FTP, and Telnet to be layered on top of it transparently.¹³

Platform Support:

UNIX and Windows NT (incorporated into Netscape commercial Web server products and Microsoft's Internet Information Server).

Industry Adoption/Standardization:

Netscape has submitted the latest version of the SSL protocol (Version 3.0, March 1996) to the IETF and it is available as an Internet Draft.¹⁴ Netscape is actively pursuing the standardization of SSL within the framework of the IETF standards process and is working with industry consortium groups to ensure that open and interoperable security standards exist now and in the future. SSL is an open, nonproprietary protocol. It has been submitted to the W3C working group on security for consideration as a standard security approach for Web browsers and servers on the Internet.

Recommendations:

Implement SSL for encryption only. This will provide data confidentiality for Web-based DD61 transactions between a client and the CECOM or AFMC TDAS servers.

7.4.3.6 Oracle Advanced Networking Option

Introduced with Oracle 7, Release 7.3, The Oracle Advanced Networking Option bundles the functionality previously provided by *Secure Network Services*, SQL*Net/Distributed Computing Environment (DCE) and SQL*Net native naming integration adapters into one product with the following features:

- Network security, authentication, and encryption services.
- Distributed computing environment integration.
- Native naming adapters for non-Oracle naming services.

The Advanced Networking Option ensures data confidentiality using RSA Data Security's RC4 or the DES encryption algorithms. Data integrity is provided by means of the MD5 message digest algorithm.¹⁵

Security Problem That Is Addressed:

Data confidentiality and data integrity over a network.

Technology Implementation Level (application, presentation, session, transport, network, link):

Session Layer.

Platform Support:

¹³ *ibid.*

¹⁴ Netscape SSL Version 3.0; Internet URL: <http://home.netscape.com/newsref/std/SSL.html>

¹⁵ Oracle Advanced Networking Option. Internet URL: <http://www.oracle.com/products/networking/html/index.html>

Any platform on which SQL*Net is supported. Windows95, Windows NT 4.0 workstation, Windows NT 4.0 Server, UNIX workstations.

Industry Adoption/Standardization:

NIST FIPS Publications 46-2 and 81: Data Encryption Standard (DES) and DES Modes of Operation, Internet Engineering Task Force (IETF) RFC 1828, IP Authentication using Keyed MD5 (standards track protocol).¹⁶

Recommendations:

For remote TDAS clients who expect to use TDAS more than 50% of daily work hours, implement the stand-alone version of TDAS with the Advanced Networking Option from Oracle. This will provide encryption of data traffic between the user's client machine and the TDAS host server (Windows NT 4.0 server on an Intel SMP platform).

7.4.3.7 Virtual Private Data Networks and Point-to-Point Tunneling Protocol

Virtual Private Data Networks (VPDN) are private data networks that utilize secure tunneling across the wide area network and typically leverage the public Internet to deliver data services for intra-company and inter-company communication. Point-to-Point Tunneling Protocol (PPTP) is a technology for securing TCP/IP traffic between Windows 95/NT clients connected to the Internet via Point-to-Point (PPP), and Windows NT servers on LANs behind corporate firewalls. It was developed by US Robotics. It is primarily being promoted by Microsoft as its Virtual Private Network (VPN) solution between a client and a server over the Internet. VPNs differ from credit card and consumer ordering transactions in that the volume of data between the two parties is greater and the two parties are well known to each other.

Security Problem That Is Addressed:

Message integrity.

Technology Implementation Level (application, presentation, session, transport, network, and link):

Network Level

Platform Support:

Microsoft: Windows 95, Windows NT 4.0 Clients, and Windows NT 4.0 servers. The current implementation depends heavily on Microsoft Windows NT Remote Access Server (RAS).

Ascend Communications and Cisco Systems: IP router products.

Digital Equipment Corporation:

Server Platforms: AltaVista Tunnel 97¹⁷ for Windows NT, Digital UNIX, and BSD.¹⁸

¹⁶ IP Authentication Using Keyed MD5, RFC 1828, IETF Network Working Group, August 1995. Internet URL: <http://www.internic.net/rfc/rfc1828.txt>

¹⁷ <http://avsoft6.pa-x.dec.com/tunnel/>

¹⁸ Source: AltaVista: <http://avsoft6.pa-x.dec.com/tunnel/showcase/analysis1/index.htm>

Client Platforms: Windows 95, Windows NT.

Checkpoint: Checkpoint Secure remote V3.0.¹⁹

Server Platforms: Windows NT, Sun/Solaris, and HP-UX.

Client Platforms: Windows 95, Windows NT.

Secure Computing: Borderware Firewall Server 5.1 with VPN Option.

Server Platforms: Proprietary OS, Intel Pentium, or Pentium Pro.²⁰

Data Fellows Ltd.: F-Secure VPN software²¹ runs on a Pentium. The package includes UNIX and the encryption engine; once loaded, it turns the machine into a security server.

Industry Adoption/Standardization:

Draft Layer 2 Tunneling Protocol (L2TP) standard submitted to IETF in Summer of 1996. This draft combined Microsoft's PPTP and Cisco's Layer 2 Forwarding (L2F), the two rival methods of sending corporate data through secure tunnels over the Internet.²² In addition, the Secure Wide Area Networking (S/WAN) initiative is an effort to provide interoperability between tunneling products. The S/WAN initiative intends to establish ground rules based on the IETF proposed IP Security Protocol (IPsec) standard²³ so that companies may mix-and-match the best firewall and TCP/IP stack products to build Internet-based VPNs.²⁴

Internet Security Recommendations:

Implement anti-virus software on both TDAS clients and server(s). Implement SSL for Web-based transactions (Web FORMS) to protect sensitive data.

7.4.4 Security Audits for Windows NT 4.0 Servers

Multiple security issues for Windows NT 4.0 server have been documented since the 4.0 production release.^{25 26 27 28} Microsoft has release service packs and other fixes to fix known flaws. Security audit software checks for known file modifications, vulnerable versions, weak passwords, common misconfigurations, and viruses. In addition to COTS products, the Department of Energy's Computer Incident Advisory Capability (CIAC) has released a free Windows NT security audit tool. Security Profile Inspector (SPI) for NT is available to the Department of Energy, the Department of Defense, and their contractors. The latest release of

¹⁹ <http://avsoft6.pa-x.dec.com/tunnel/showcase/analysis4/index.htm>

²⁰ Secure Computing: http://www.securecomputing.com/P_FWall_BWF_FRS.html

²¹ http://www.data.com/hot_products/software_security/fellows.html

²² Paone, Joe "Microsoft's PPTP and Cisco's L2F proposed standards to merge", LAN Times, October 14, 1996. Internet URL: <http://www.wcmh.com/lantimes/96oct/610a046a.html>

²³ VPN's use tunneling to Build Private Business Links, Datamation, June 1996. Internet Source: <http://www.datamation.com/PlugIn/issues/1996/june1/06ainet3.html>

²⁴ RSA Labs Security FAQ, Q137. <http://www.rsa.com/rsalabs/newfaq/q137.html>

²⁵ Computer Security Institute's Alert Newsletter,(October 1996)

²⁶ Windows NT Security FAQ, version 3.0. September 11, 1997. <http://www.iss.net/vd/ntfaq.html>

²⁷ Red Button Bug. <http://ntsecurity.com/RedButton/default.htm>

²⁸ Windows NT 4.0 Server Service Pack 3 Security Enhancements. <http://www.microsoft.com/ntserver/guide/secenhance.asp?A=2&B=10>

SPI for NT includes numerous user interface enhancements, bug fixes, native Windows online Help, new reference manual, and verification of Year 2000 compliance.²⁹

Security Audit Recommendation: Acquire SPI for NT from the Department of Energy CIAC and periodically run the software on the TDAS Windows NT server. Monitor CIAC's Web site for updates to the SPI for NT.

7.5 Database Schema Design

General database schema design practice will be implemented for the TDAS. However, the design of database schema will take into account the following factors:

- The legacy data that can be extracted correctly and cost-effectively from various media.
- The degree of modifications to the layout of DD Form 61 in process.
- Any changes to the current process at each MSTDS and external client sides.

Because the design of the DD Form 61 predicated the development of modern database software and network hardware, the conversion of legacy data is a major challenge. Therefore, based on the DD Form 61 format, the TDAS will not fully take advantage of abilities in a RDBMS. The database schema design will be implemented based on the current business process and usage of the current DD61 form. Any future consideration for changes (in the DD Form 61) will be addressed at that time.

7.6 TDAS Help Design

The TDAS Help system will be crafted with the user in mind. It is a given that members of the TDAS-user audience already know how to do their respective jobs. The TDAS Help system will be designed to provide for the user a reference source that can answer the sort of "what happens if I..." questions that are asked by users when learning to use unfamiliar software, or even when accessing little-used features of familiar software. The TDAS Help system will provide information about the nature and purpose of every element of the TDAS user-interface, including all of the DD Form 61's fields and all of the interface's available commands.

The TDAS Help system will be developed using RoboHelp v.5.0. This will ensure that our Help systems can be created and maintained with a minimum of effort and uncertainty. RoboHelp uses MS Word for Windows, and is among the two or three best tools available for the development of Help systems.

²⁹ DOE Computer Incident Advisory Capability, Security Profile Inspector for NT.
<http://ciac.llnl.gov/cstc/spi/spiwnt/spiwnt.html>

APPENDIX A: REFERENCES

“Draft Operational Concept Description for the Type Designator/Federal Logistics Information System Interface,” LITTON/PRC, December 31, 1996.

“Web Application Development Tools, Sorting the Strategies,” *InfoWorld*, February 24, 1997, Volume 19, Issue 8.

National Computer Security Association (NCSA) Web page: www.ncsa.com.

Ascend Firewall 101: Internet URL: <http://www.ascend.com/861.html>

Introduction to SOCKS, <http://www.socks.nec.com/introduction.html>

SOCKS FAQ, Internet URL: <http://www.socks.nec.com/socksfaq.html#q12>

[http://www.globecom.net/\(nobg,sv\)/ietf/rfc/rfc1929.shtml](http://www.globecom.net/(nobg,sv)/ietf/rfc/rfc1929.shtml)

RSA Security Solutions Catalog: http://www.rsa.com/rsa/PRODUCTS/sscat_winter96/97wor/index.html

RSA Laboratories PKCS: <http://www.rsa.com/rsalabs/pubs/PKCS/>

SSL Reference Document, Netscape Communications: <http://home.netscape.com/info/security-doc.html>

RSA Labs Security FAQ: <http://www.rsa.com/rsalabs/newfaq/q134.html>

Netscape SSL Version 3.0; Internet URL: <http://home.netscape.com/newsref/std/SSL.html>

<http://avsoft6.pa-x.dec.com/tunnel/>

Source: AltaVista: <http://avsoft6.pa-x.dec.com/tunnel/showcase/analysis1/index.htm>

<http://avsoft6.pa-x.dec.com/tunnel/showcase/analysis4/index.htm>

Secure Computing: http://www.securecomputing.com/P_FWall_BWF_FRS.html

http://www.data.com/hot_products/software_security/fellows.html

Paone, Joe “Microsoft's PPTP and Cisco's L2F proposed standards to merge”, LAN Times, October 14, 1996. Internet URL: <http://www.wcmh.com/lantimes/96oct/610a046a.html>

VPN's use tunneling to Build Private Business Links, Datamation, June 1996. Internet Source: <http://www.datamation.com/PlugIn/issues/1996/june1/06ainet3.html>

RSA Labs Security FAQ, Q137. <http://www.rsa.com/rsalabs/newfaq/q137.html>

APPENDIX B: ACRONYMS AND ABBREVIATIONS

4GL	Fourth-Generation Language
ALR	Advanced Logic Research
AFMC	Air Force Material Command
AFT	Authenticated Firewall Traversal
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CAGE	Commercial and Government Entity
CALS	Continuous Acquisition and Life-cycle Support
CDRL	Contract Data Requirements List
CECOM	Communication and Electronic Command
CIAC	Computer Incident Advisory Capability
CONOPs	Concept of Operations
COTS	Commercial Off-The-Shelf
DBMS	Database Management System
DCE	Distributed Computing Environment
DCP	Department Control Point
DES	Data Encryption Standard
DLSC	Defense Logistics Service Center
DoD	Department of Defense
DoDCP	Department of Defense Control Point
DSS	Digital Signature Standard
EDA	Enterprise Data Access
EDI	Electronic Data Interchange
FAQ	Frequently Asked Questions
FIPS	Federal Information Processing Standard
FLIS	Federal Logistics Information System
FTP	File Transfer Protocol
GB	Gigabytes
GSS	Generic Security Service
GUI	Graphical User Interface
HP	Hewlett Packard
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol

IDE	Integrated Data Environment
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	IP Security Protocol
ISP	Internet Service Provider
JDBC	Java Database Connectivity
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MIME	Multi-purpose Internet Mail Extensions
MSTDS	Military Service Type Designation System
NCSA	National Computer Security Association
NIST	National Institute of Standards and Technology
NNTP	Network News Transfer Protocol
NSN	National Stock Numbers
OSI	Open System Interconnect
PKC	Public Key Cryptography
PKCS	Public Key Cryptography Standards
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RAD	Rapid Application Development
RAS	Remote Access Server
RDBMS	Relational Database Management System
RFC	Request for Comments
RSA	RSA Data Security Inc.
S/WAN	Secure Wide Area Networking
S2K	System 2000
SMP	Symmetric Multi-Processor
SPI	Security Profile Inspector
SQL	Structured Query Language
SRN	Source Request Number
SSL	Secure Socket Layer
TCP	Transport Control Protocol
TDAS	Type Designation Automated System

URL	Uniform Resource Locator
USAF	United States Air Force
VPDN	Virtual Private Data Network
VPN	Virtual Private Network
W3C	W3 Consortium
WAN	Wide Area Network
WWW	World Wide Web

APPENDIX C: GLOSSARY

DoD Control Point/SuperClients	DoD control points, are the official DoD assigning agency responsible for assigning type designations within the TDAS system at CECOM, and locally use the TDAS system to formally accept or reject a type designation action received from the Department Control Points.
External Clients	Users of the TDAS system external to CECOM that include: Department Control Points, Government Agencies, and both contractors.
Department Control Points	Department control points are the official control points within the military departments authorized to obtain joint electronic type designations from the DoD Control Point. This is done externally using the TDAS system to pre-approve or reject a type designation action received that is received from a Manufacturing Contractor.
Contractors	Contractors may consist of either manufacturing or administrative. They may submit requests for type designation actions as directed by the procuring activity.
Manufacturing Contractors	The contractor responsible for actually manufacturing the particular configuration item/system that is being processed for type designation and nomenclature. This type of contractor has submittal privileges, as well as viewing privileges for data that they have submitted.
Administrative Contractors	Users who render an administrative service to Government agencies by gathering information. This type of contractor can only view approved DD61s. They have no submittal privileges and cannot view pending submittals. Administrative Contractors can only view approved submittals, however they can view any approved submittals.
Packages	A group of DD61s for a particular configuration item/system, which consists of the related sub items/systems, that is being processed for type designation and nomenclature.
Source Request Number	<p>A serial number assigned by the Department Control Point in an approved format. No two DD Form 61s may have the same SRN, whether they are a new assignment, revision, or cancellation. This also includes re-submittals of items returned without action and/or are disapproved.</p> <p>The new format of the SRN is: aaa-bb-cccc-ddd-eee</p> <p>Where: 'aaa' = 2-6 alphanumeric characters (indicates contractor) 'bb' = 2-digit year 'cccc' = sequential item number for this contractor in this year</p>

'ddd' = sequential item number for this item within a package
'eee' = total number of items in this package

Example #1:

SRN = 'DND-97-0129-005-100'

DND = contractor code

97 = year

0129 = 129th item submitted by contractor this year 005 = 5th item in this package

100 = 100 items in this package

Example #2:

SRN = 'DND-97-0141-001-001'

DND = contractor code

97 = year

0141 = 141st item submitted by contractor this year

001 = 1st item in this package

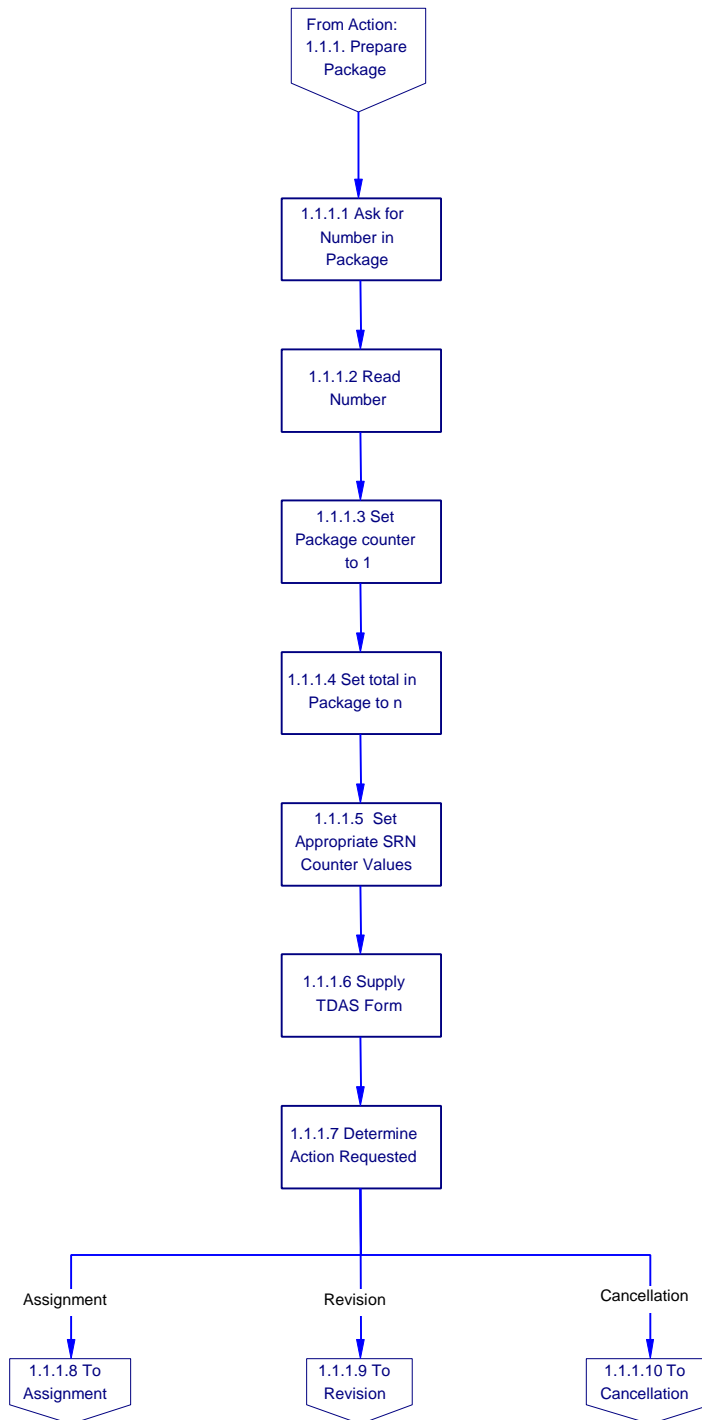
001 = 1 item in this package

Note that the last 6 digits are required, even if the submission is not part of a package.

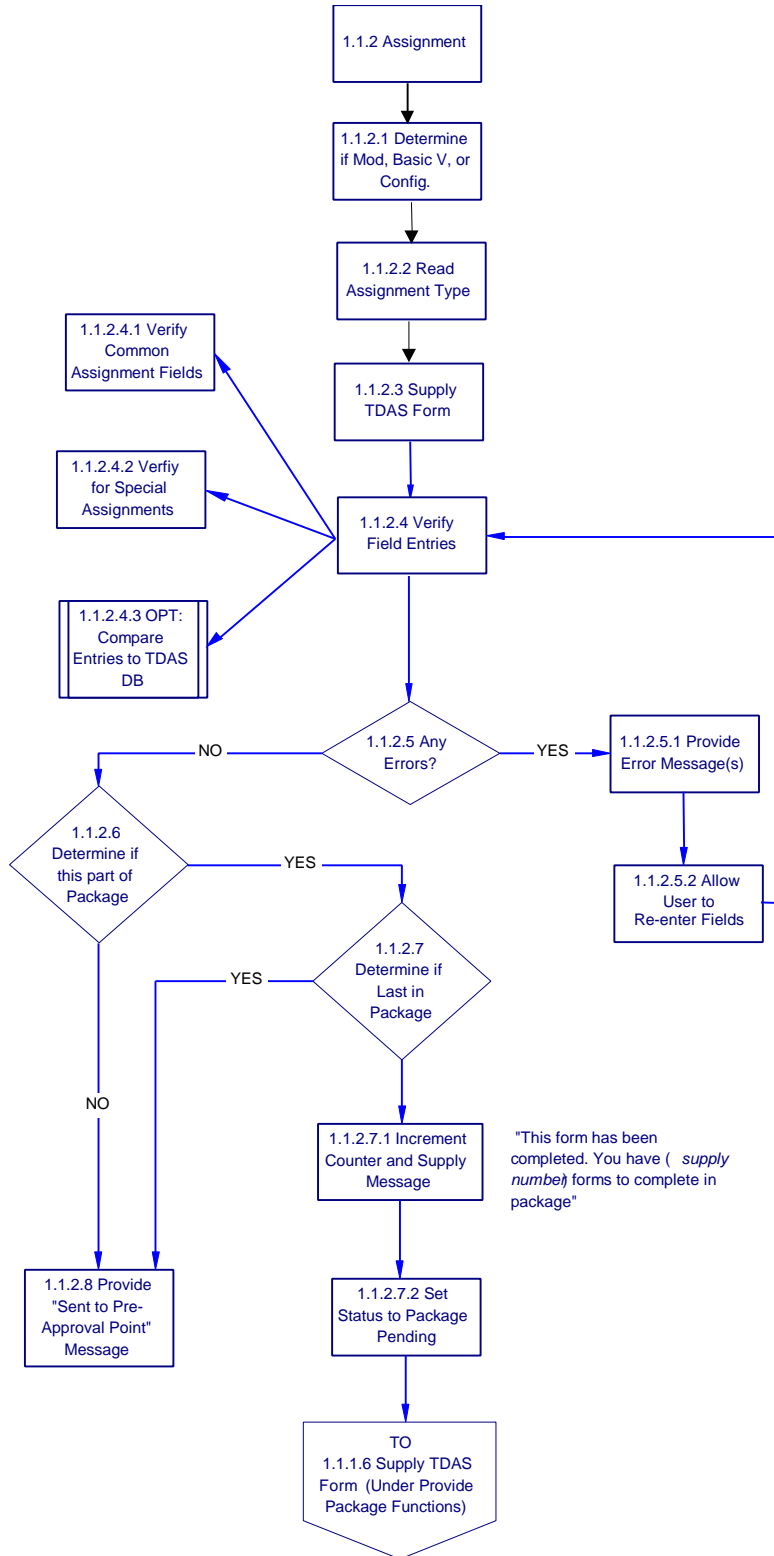
Type Designation	A combination of letters and numerals arranged in a specific sequence to provide a short significant method of identification.
Item Name	A name published in the Federal Cataloging Handbook H6, or that name developed by the requester in accordance with DoD-STD-100, that portion applicable to drawing titles. Item names used with type designation assignments will be consistent with policies of the Federal Cataloging Program.
Complement Data	A list of the major components in the item/system being nomenclatured. Note that these listed items/systems are commonly nomenclatured also. Each component listed contains the following four information fields: Quantity, Item Name, CAGE Code, and Part Number or Drawing Number (if nomenclatured designation). NSN is also available. This information is contained in item #7 of block #14 of the DD Form 61.
Ledger Book	A written record of all items that have been nomenclatured and assigned a type designation, which is used to determine the proper naming sequence for the next nomenclature and type designation. The electronic version of the ledger book will use the following key data fields from the DD61 information: Type Designation, Item Name, SRN, Type of Action, Date of Action, and Security Class.

APPENDIX D: FUNCTIONAL FLOWS

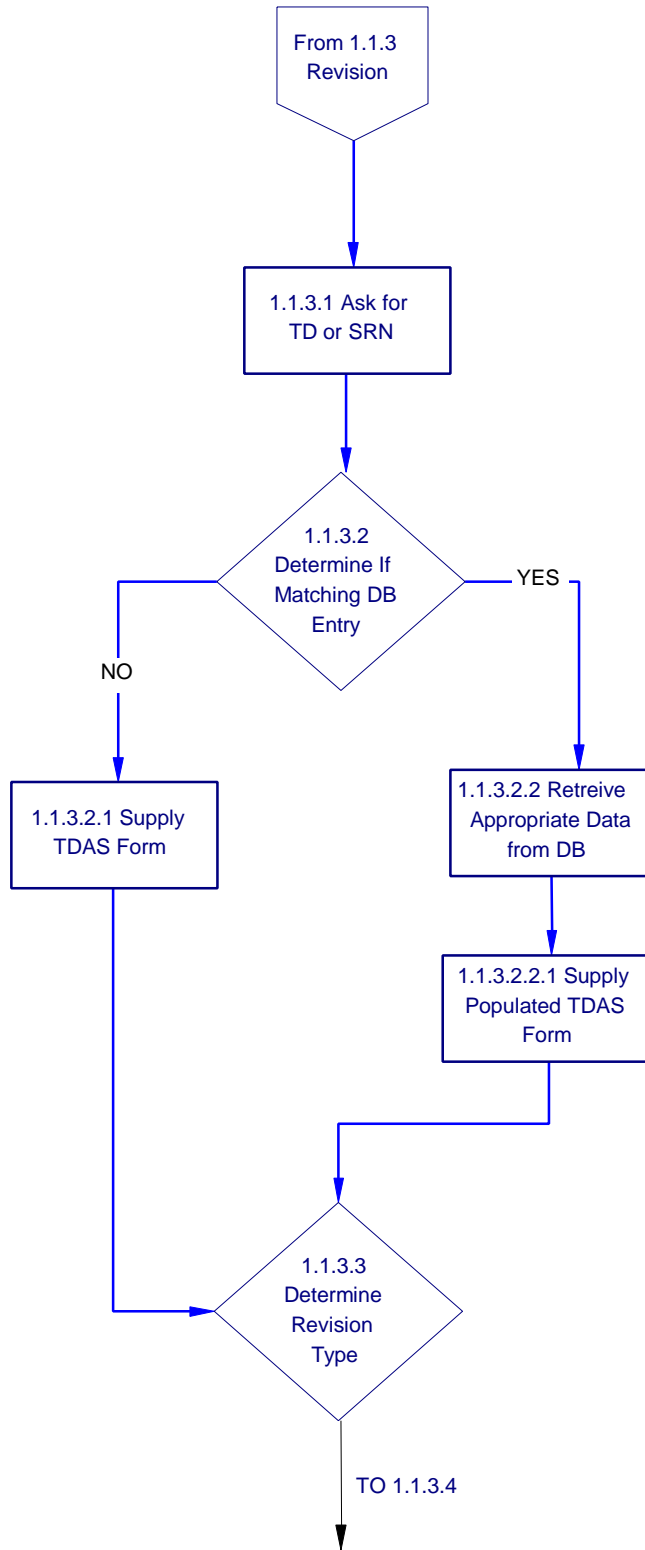
1.1.1 Prepare Package (Manufacturing Contractor)



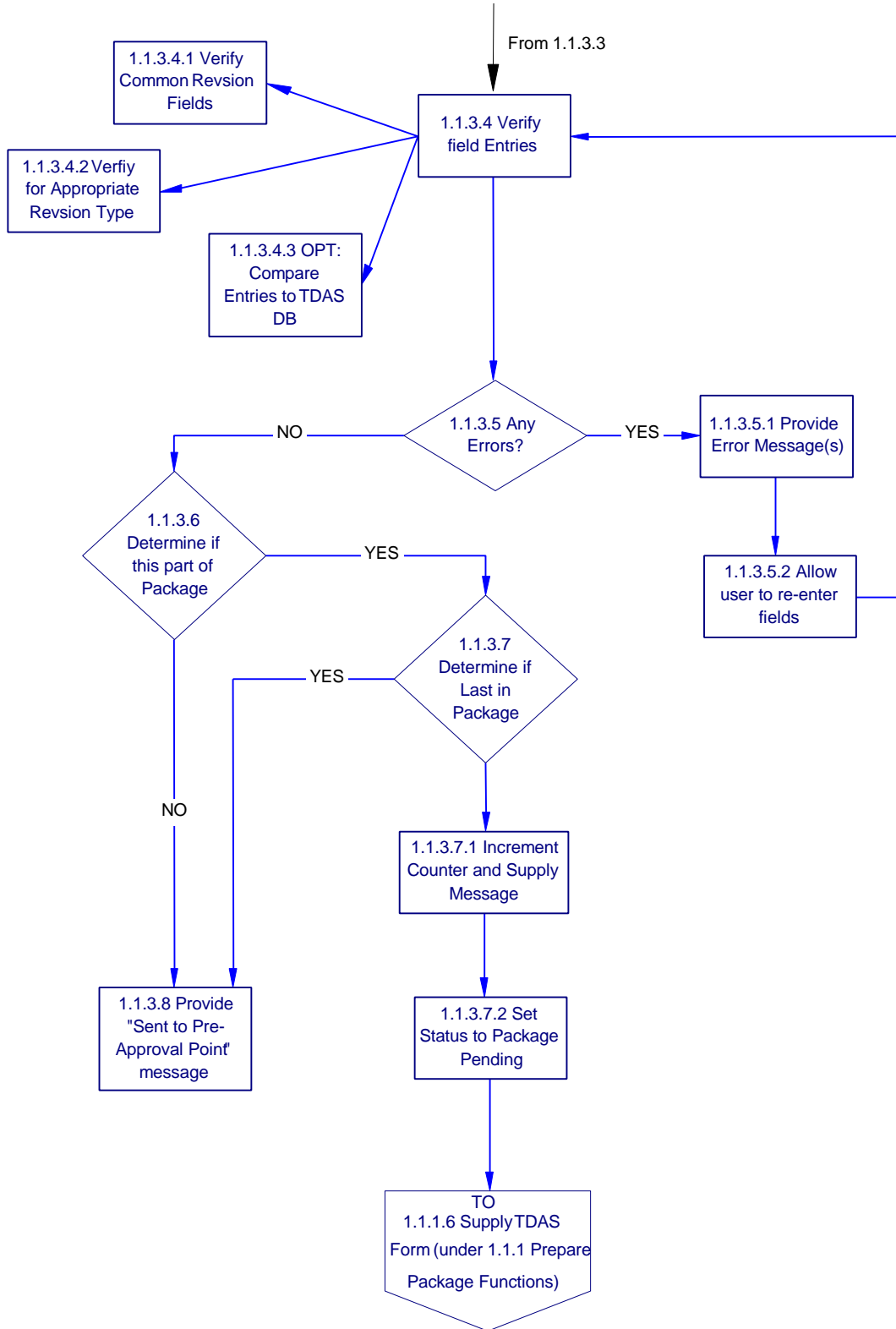
1.1.2 Assignment (Manufacturing Contractor)



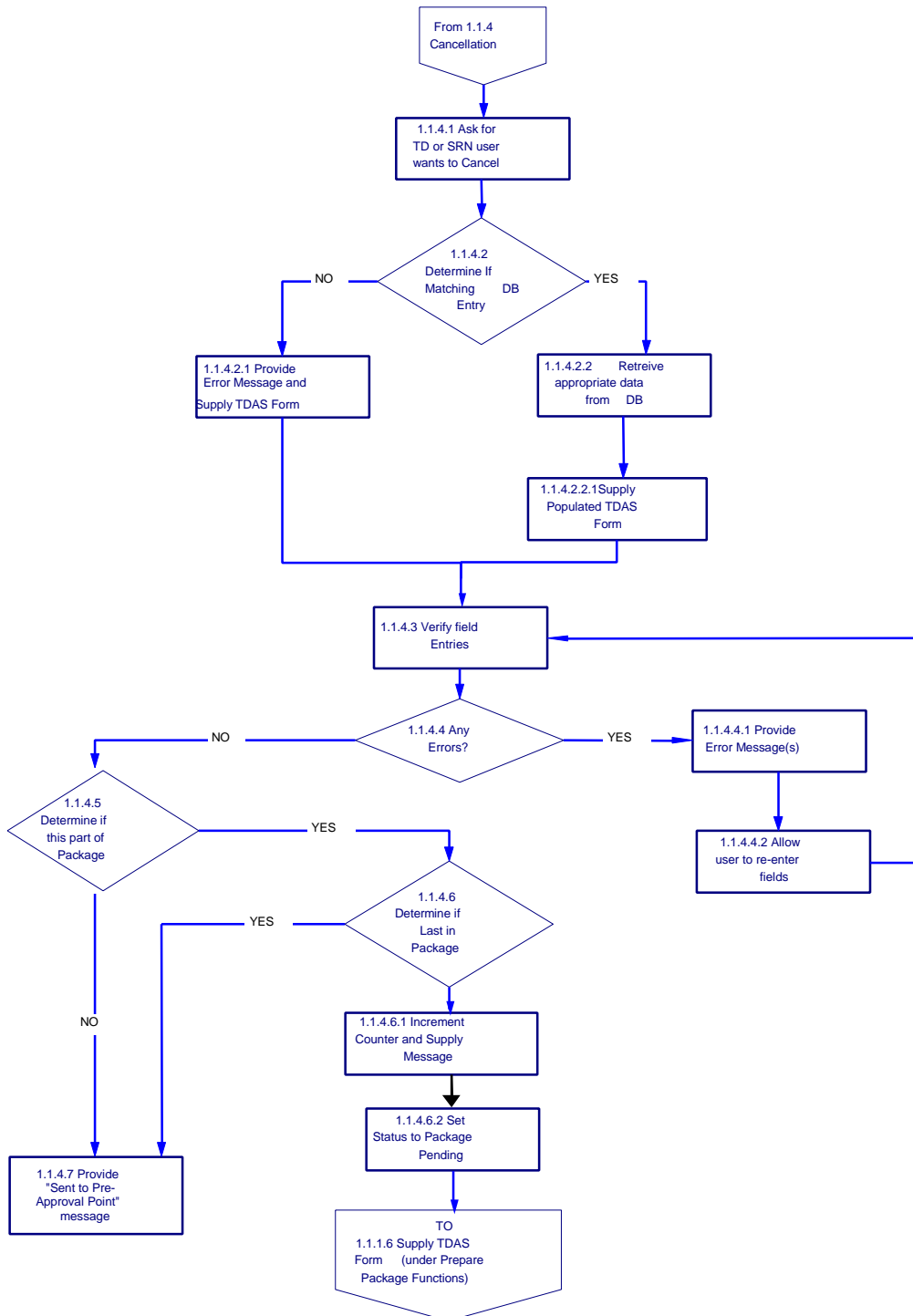
1.1.3 Revisions (Manufacturing Contractor)



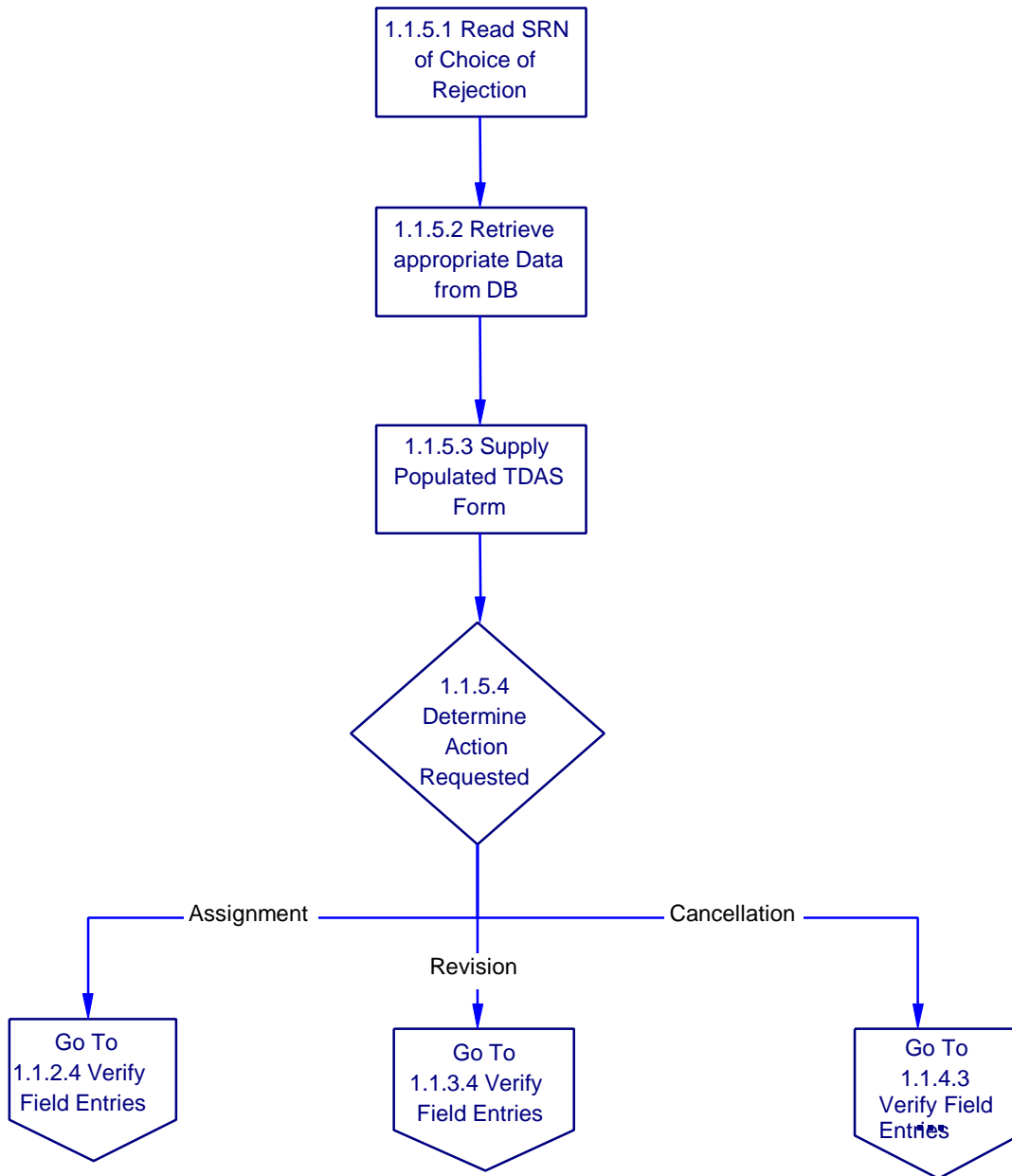
1.1.3 Revisions (continued) (Manufacturing Contractor)



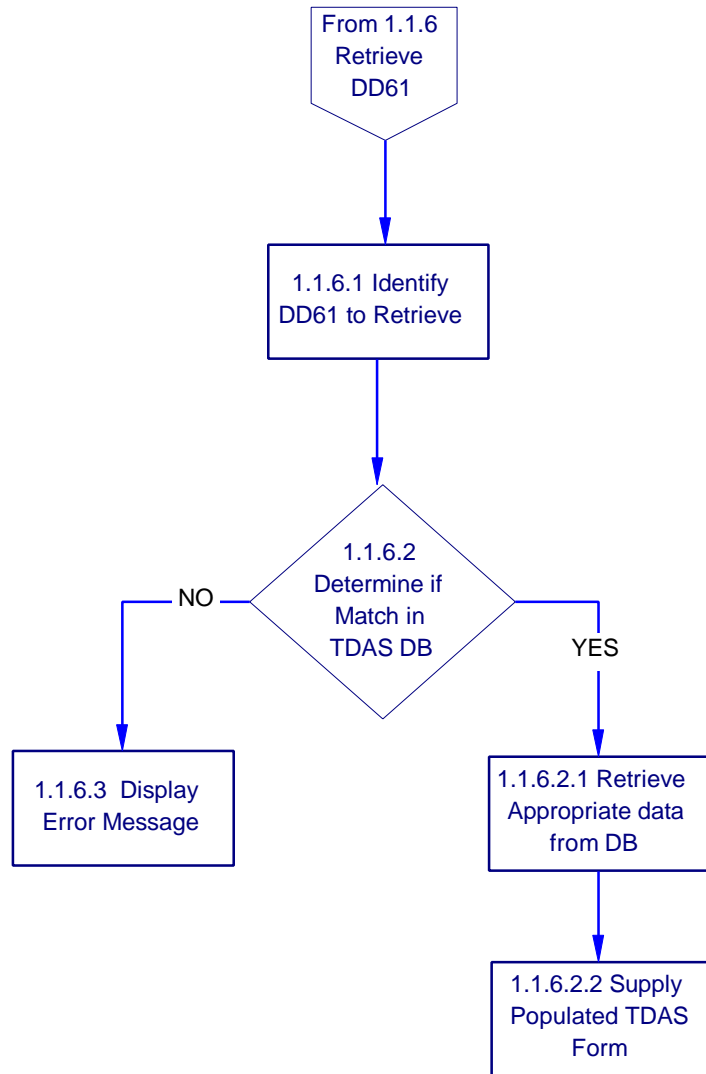
1.1.4 Cancellation (Manufacturing Contractor)



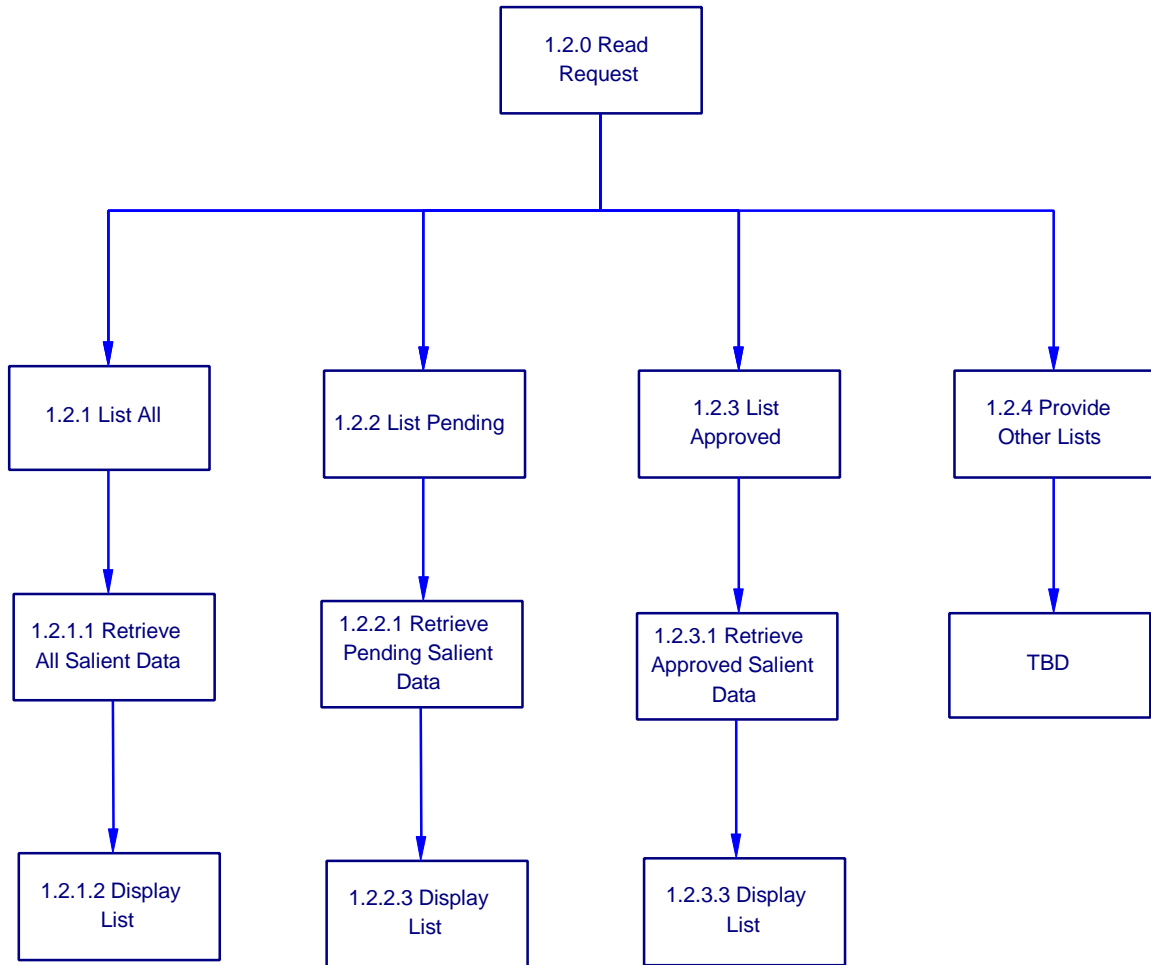
1.1.5 Modify a Rejection (Manufacturing Contractor)



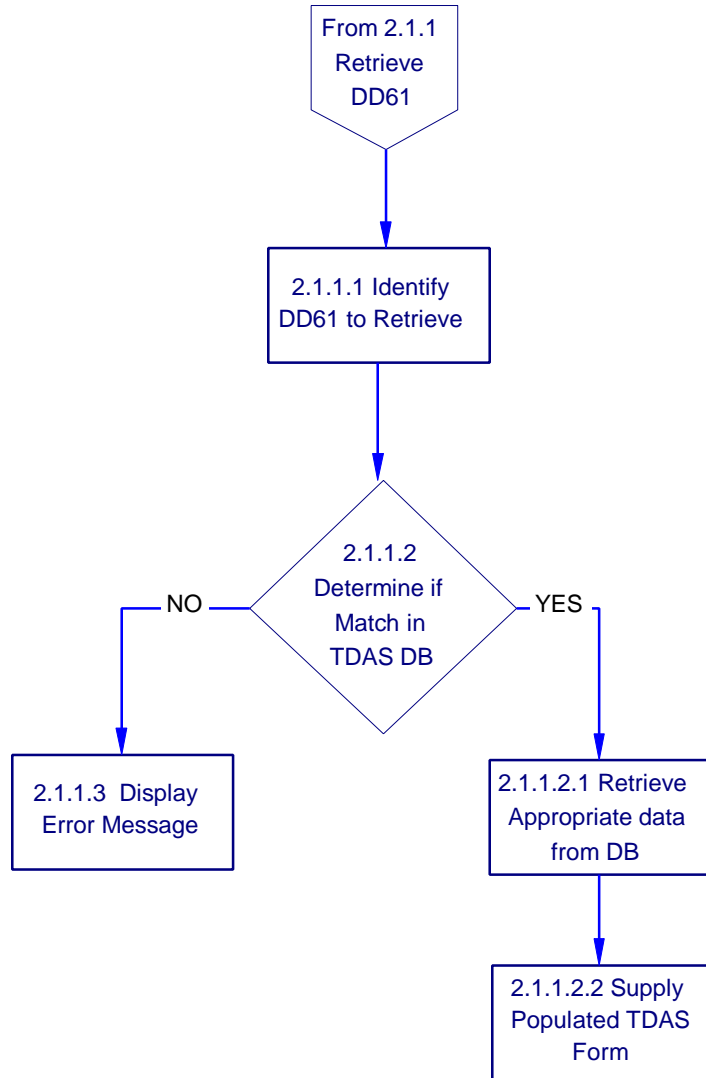
1.1.6 Retrieve a DD61 (Manufacturing Contractor)



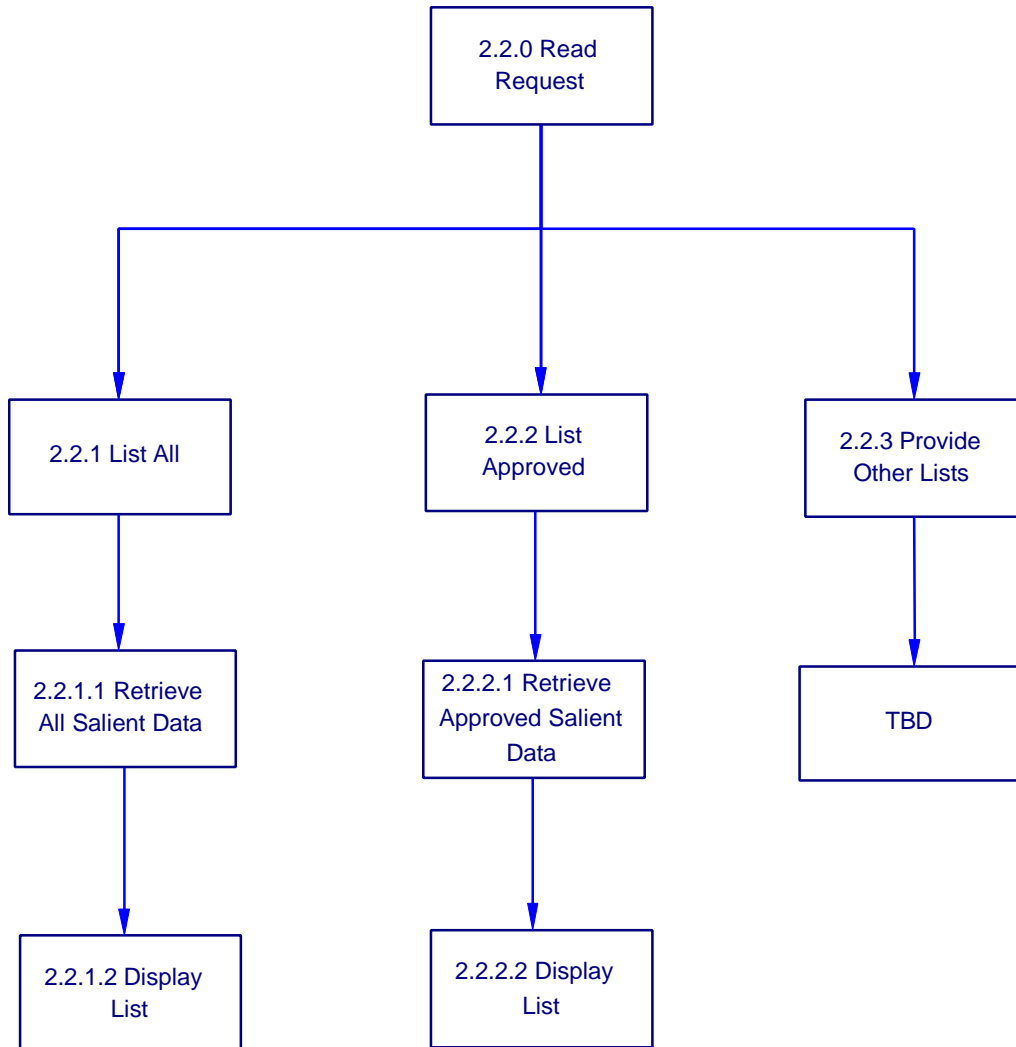
1.2 Reports (Manufacturing Contractor)



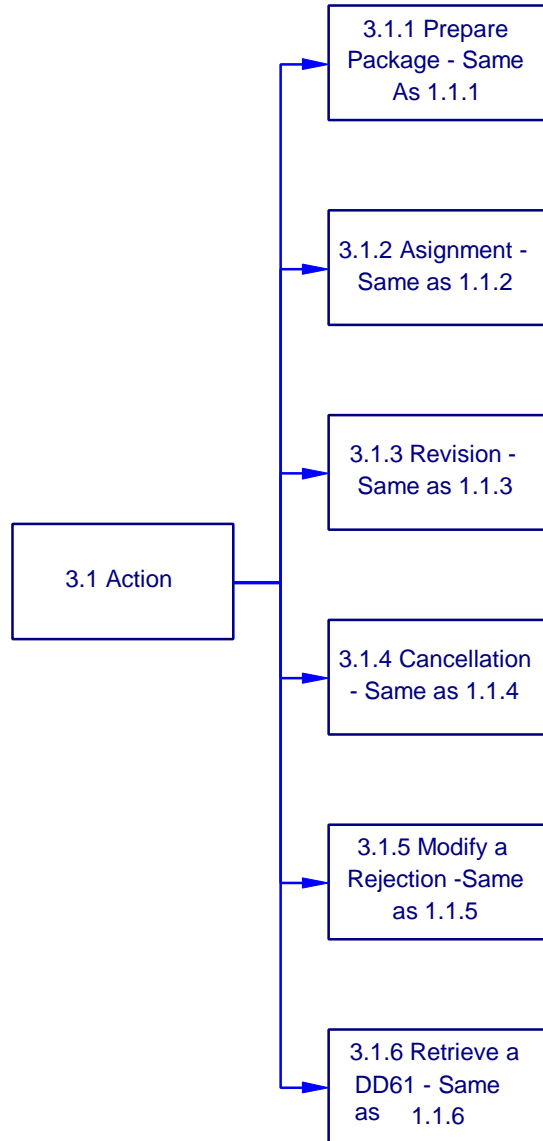
2.1.1 Retrieve DD61 (Administrative Contractor)



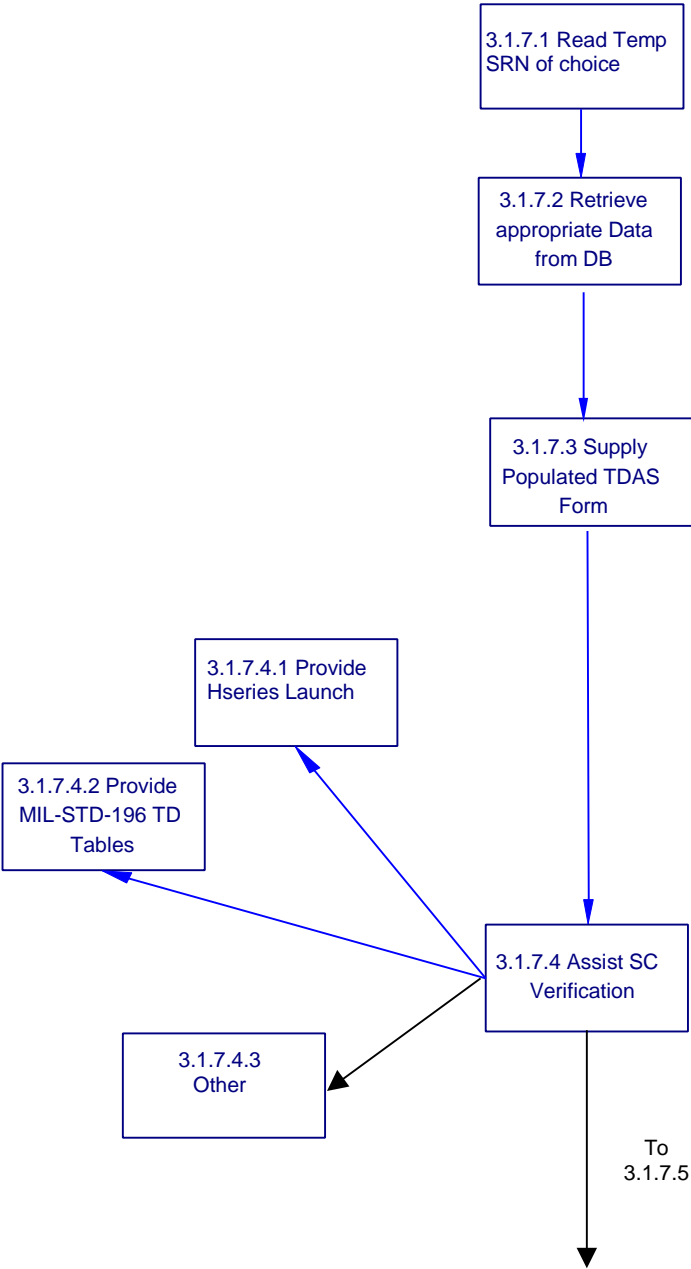
2.2 Reports (Administrative Contractor)

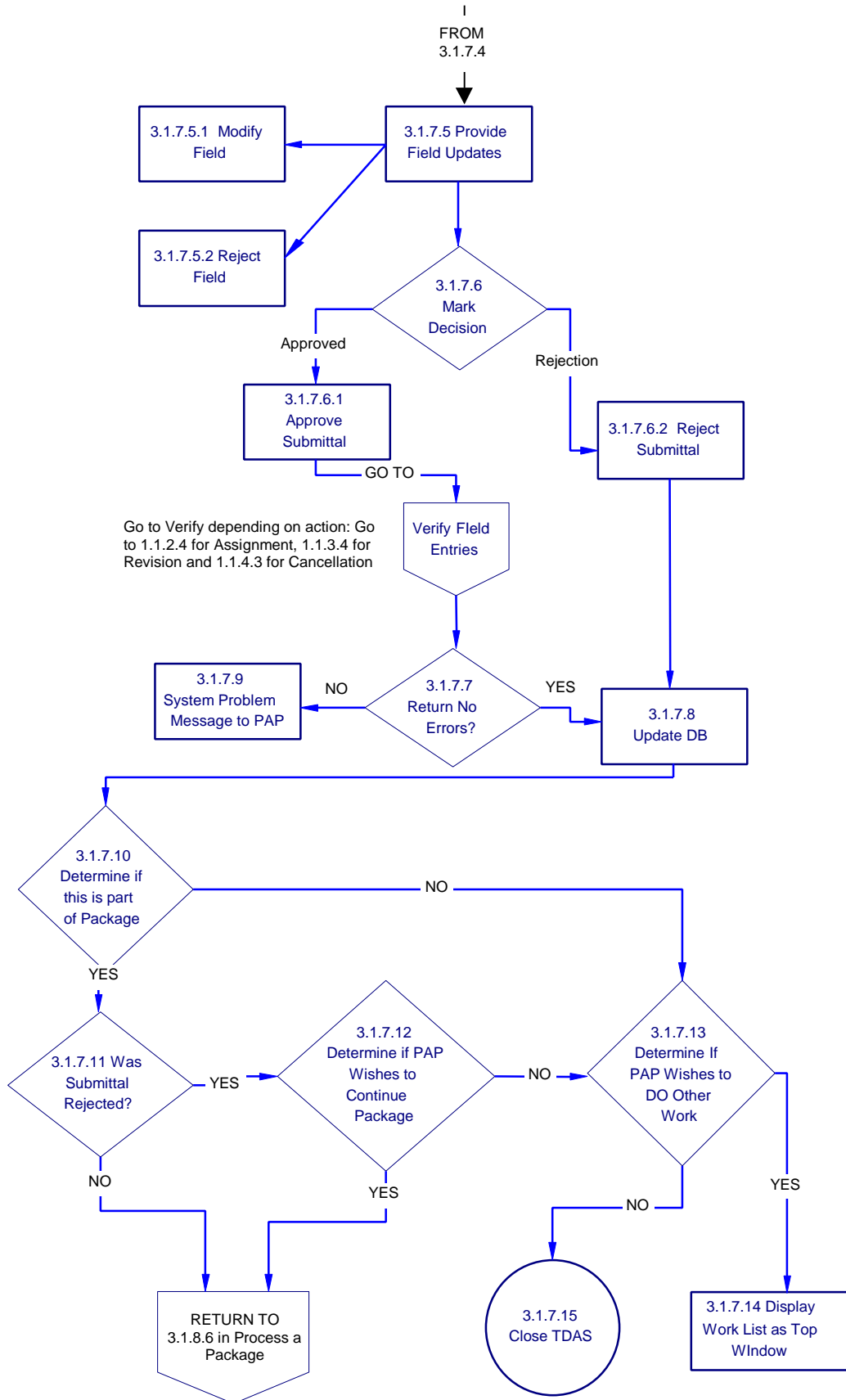


3.1.1 to 3.1.6 Actions (Department Control Point/Government Agency)

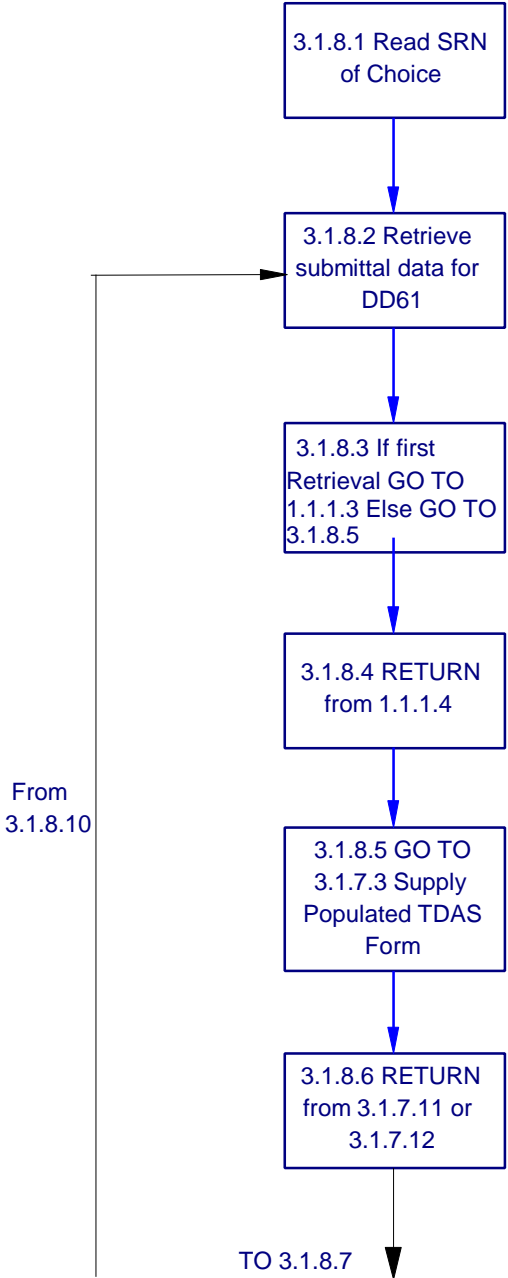


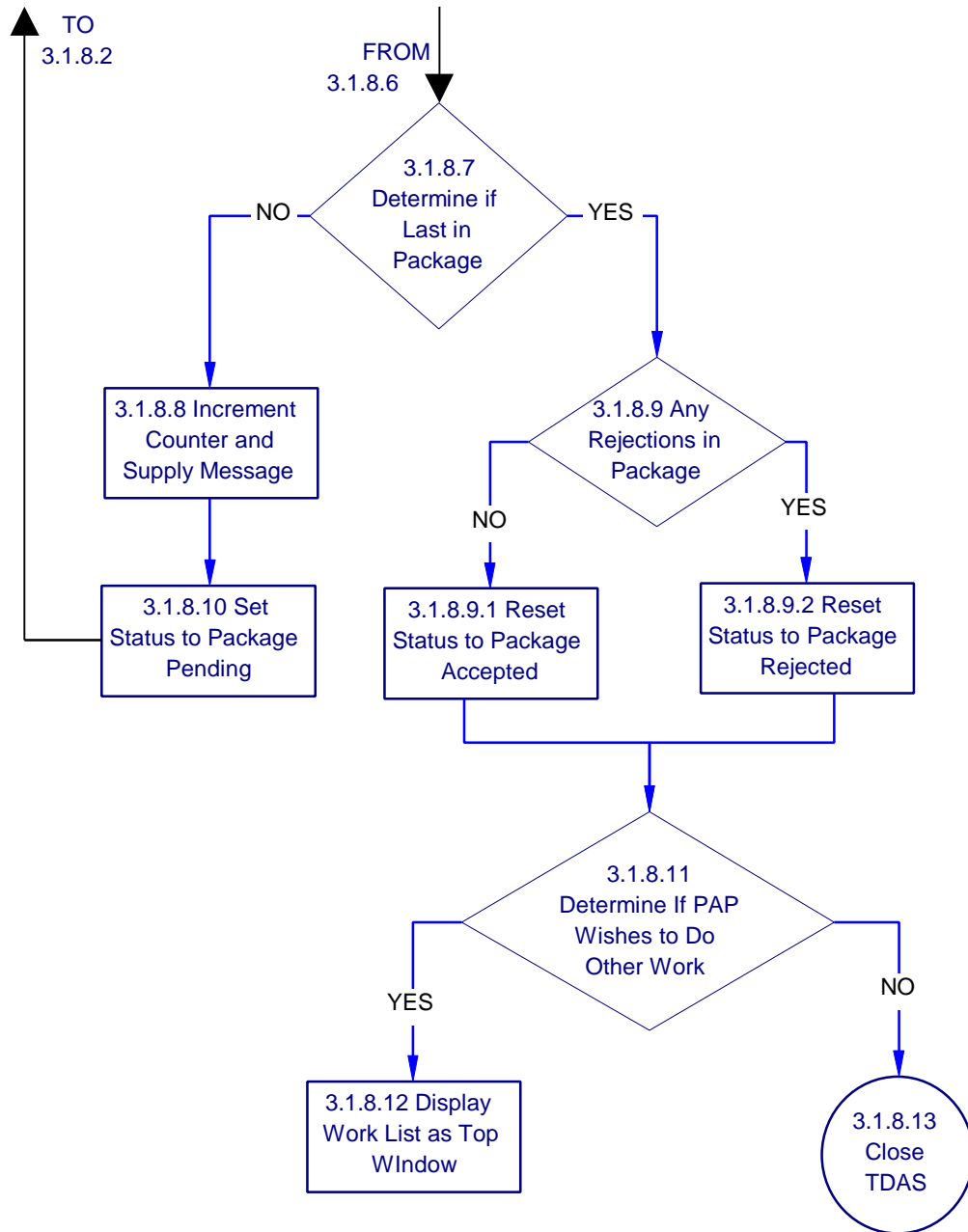
3.1.7 Process a Submittal (Department Control Point/Government Agency)



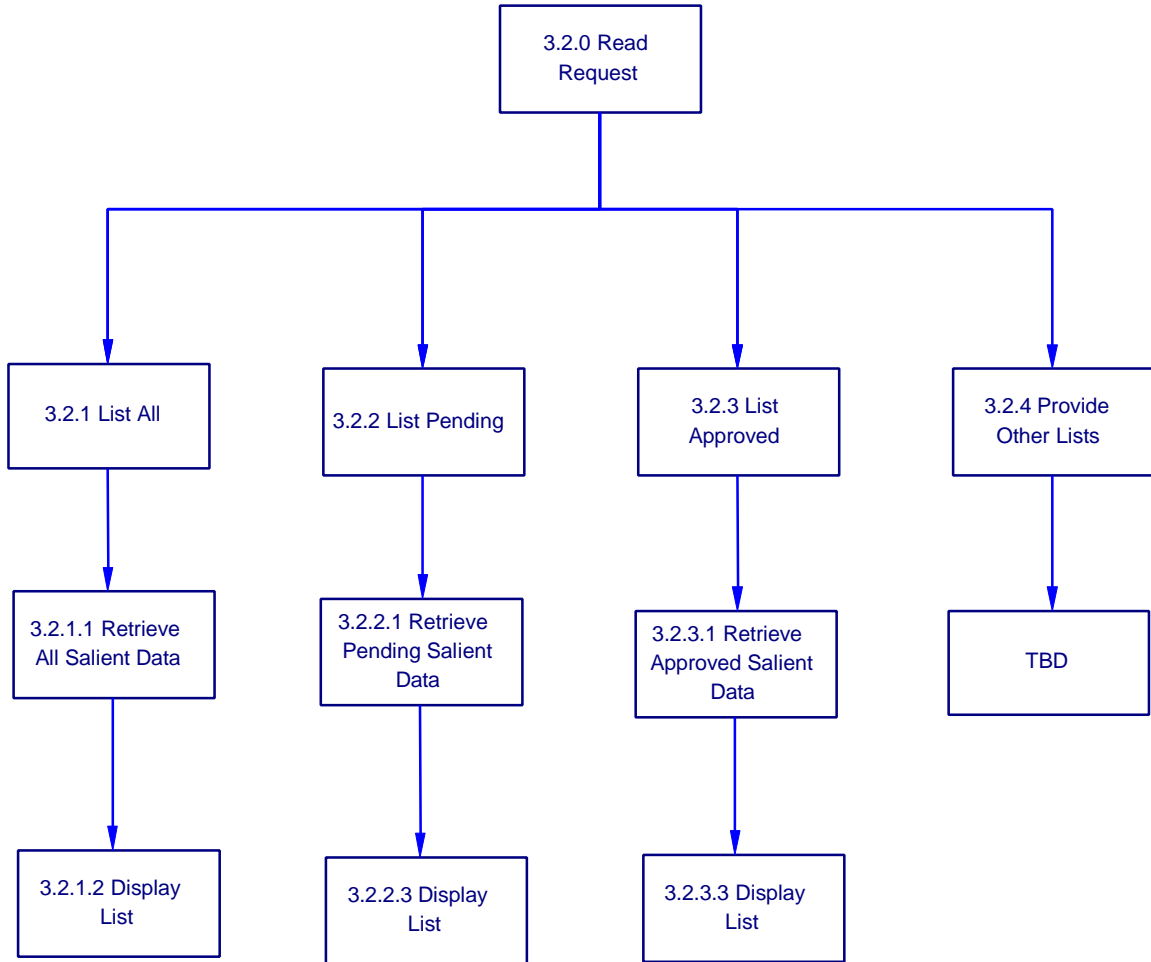


3.1.8 Process A Package (Department Control Point/Government Agency)

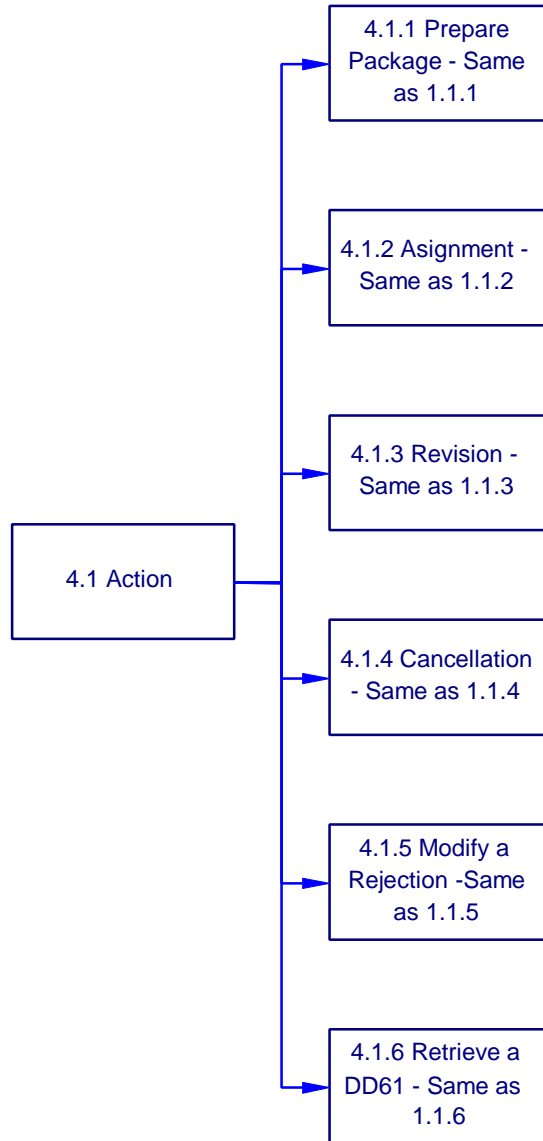




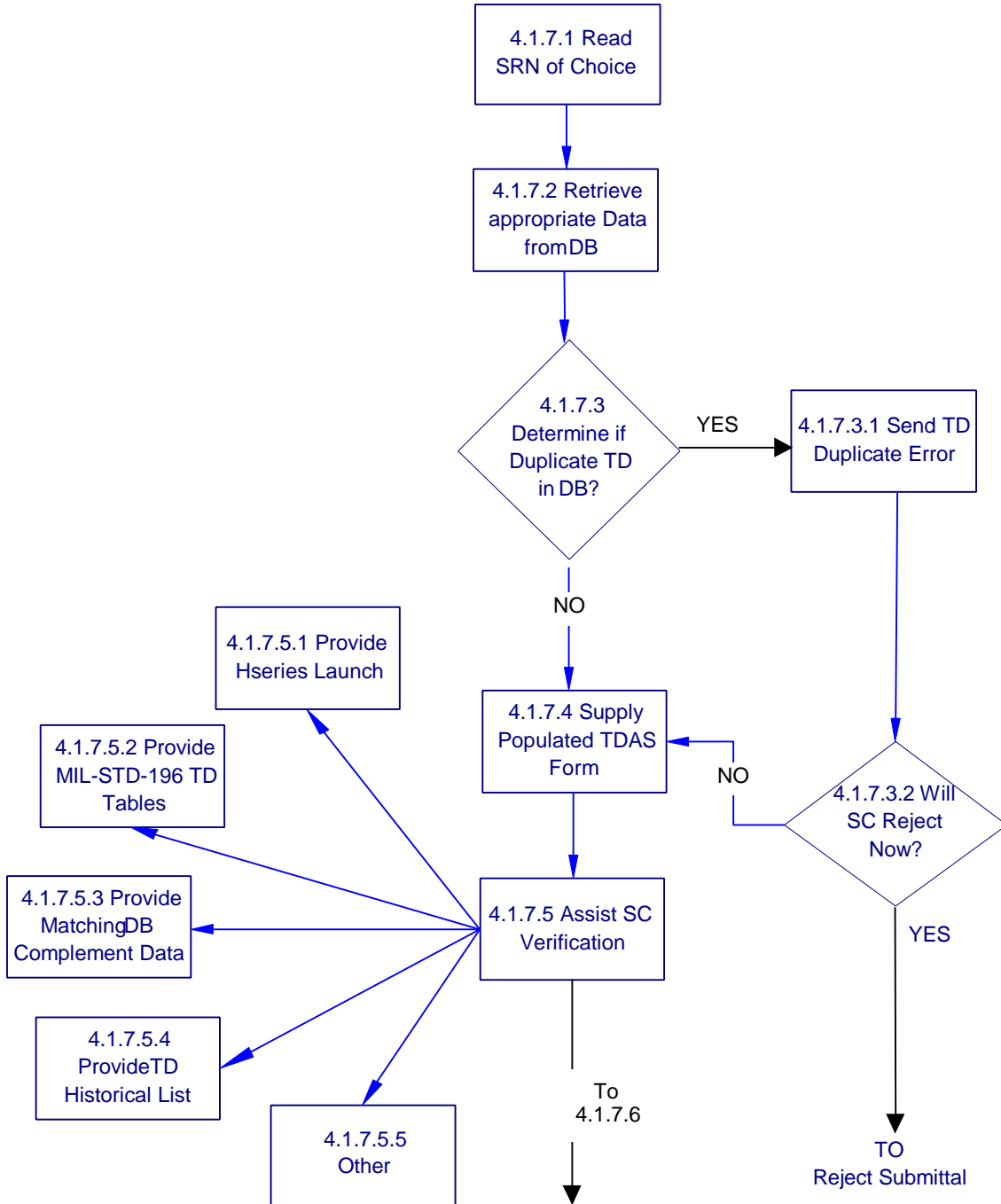
3.2 Reports (Department Control Point/Government Agency)

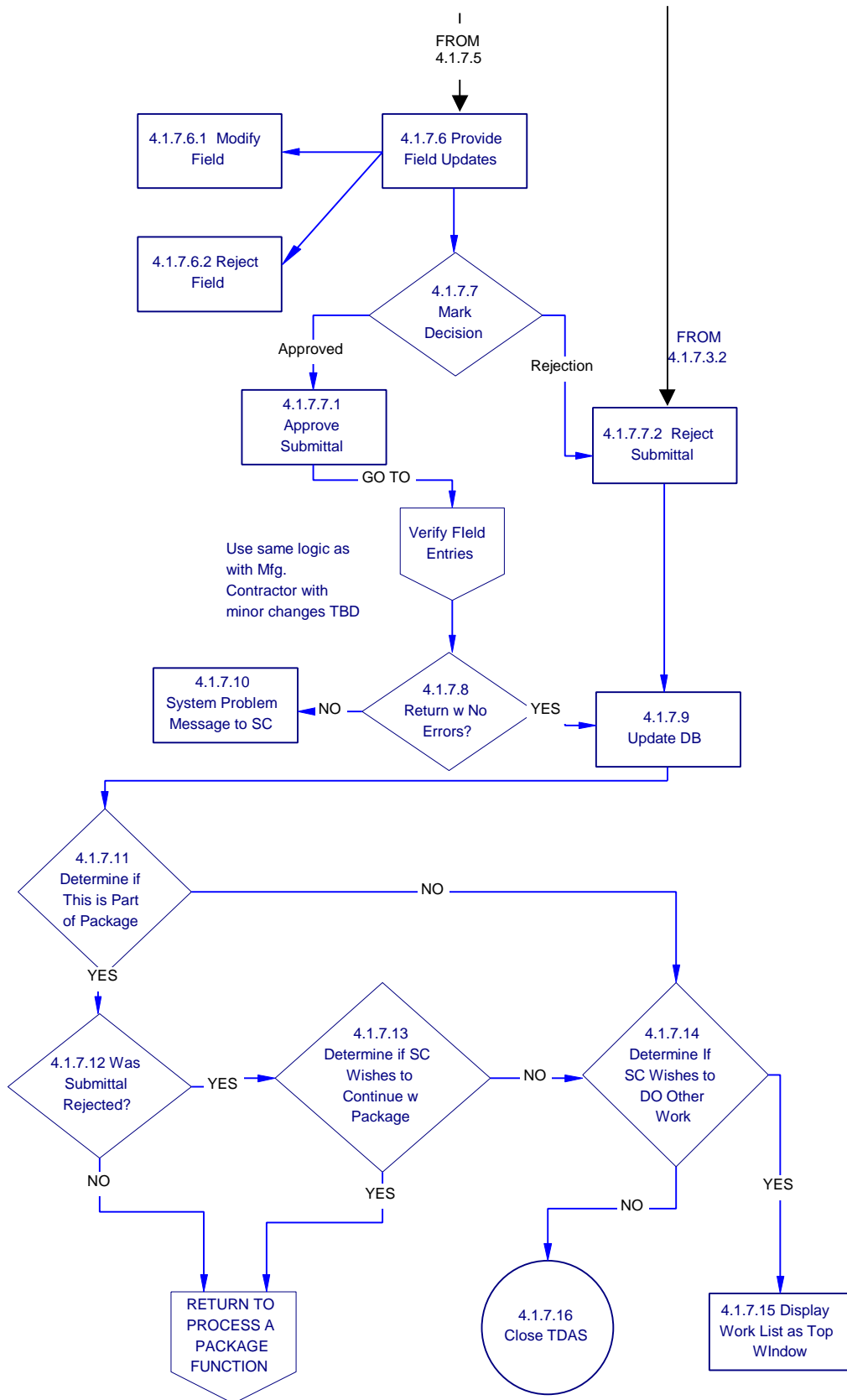


4.1 Actions (DoD Control Point)

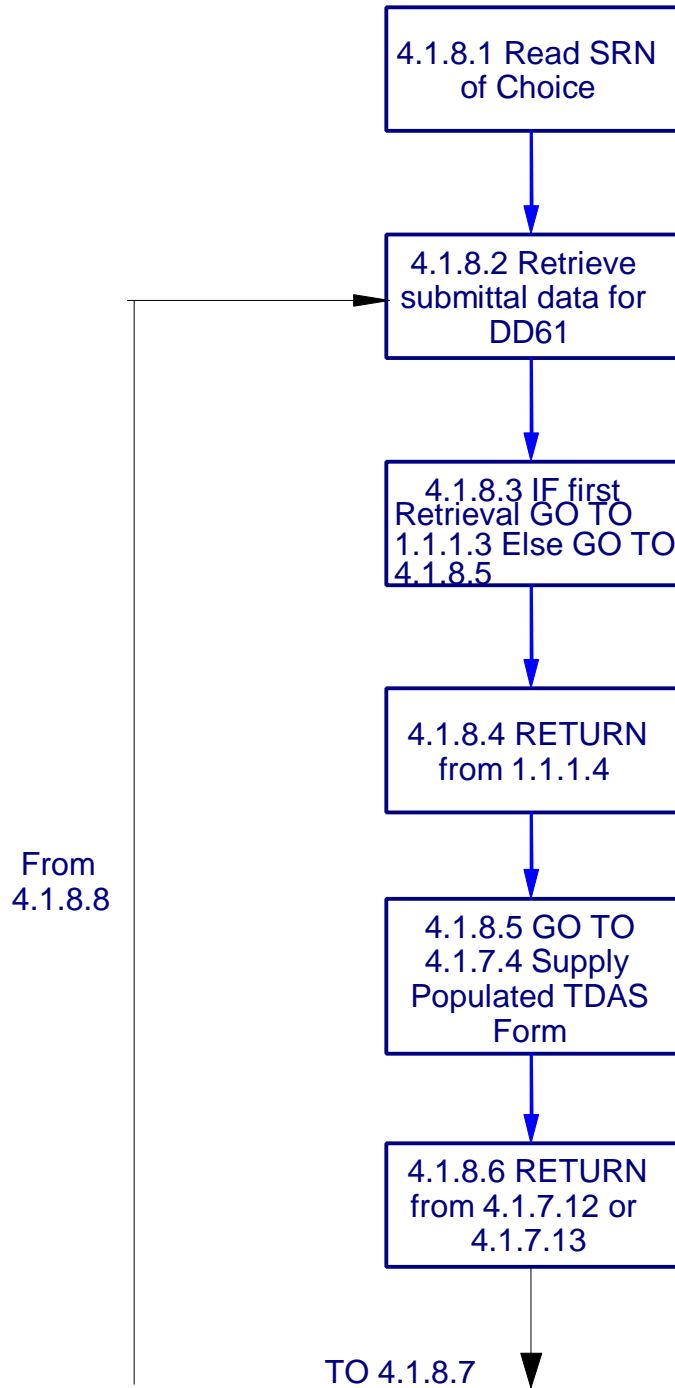


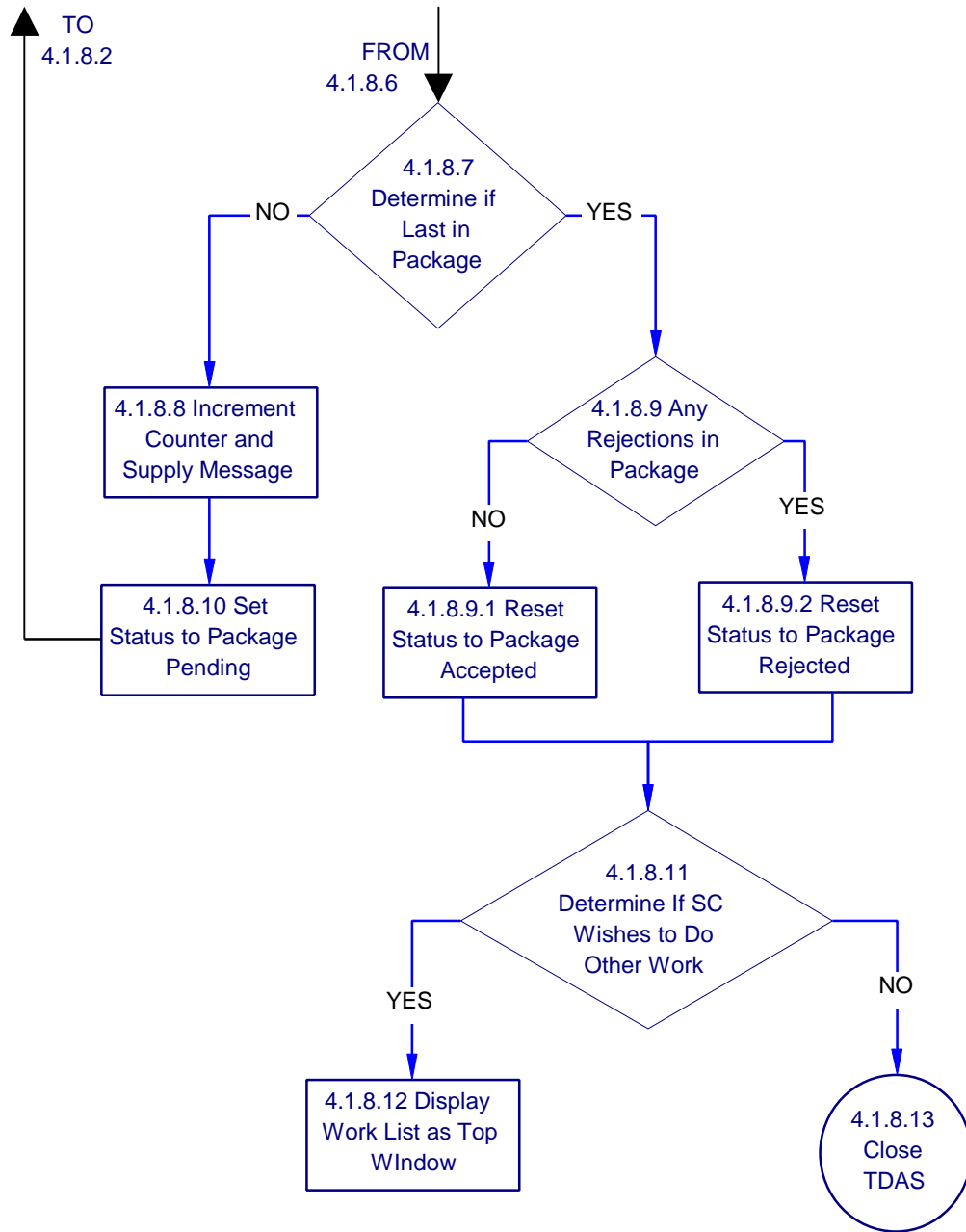
4.1.7 Process a Submittal (DoD Control Point)



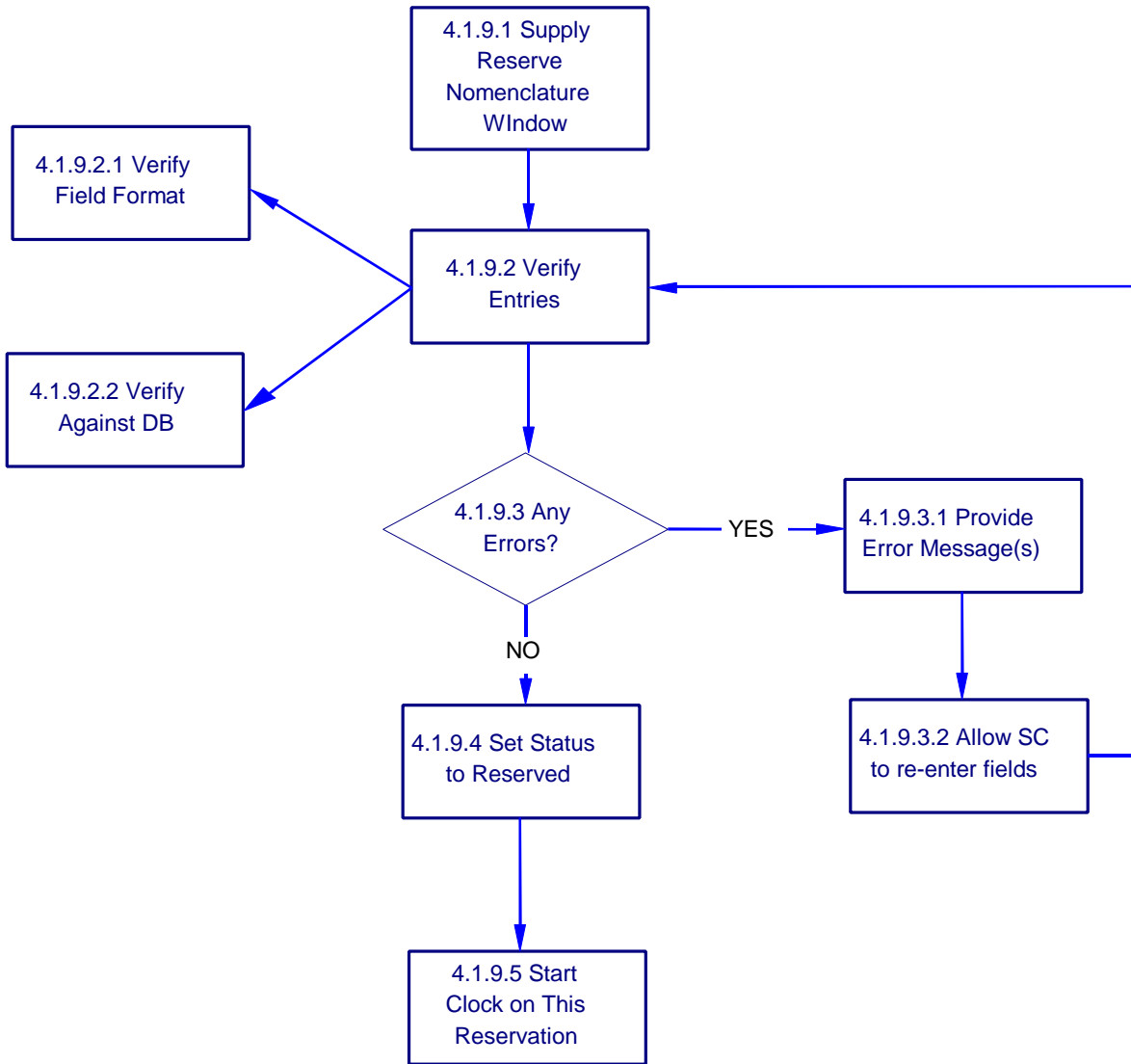


4.1.8 Process A Package (DoD Control Point)





4.1.9 Reserve Nomenclature (DoD Control Point)



4.2 Reports (DoD Control Point)

