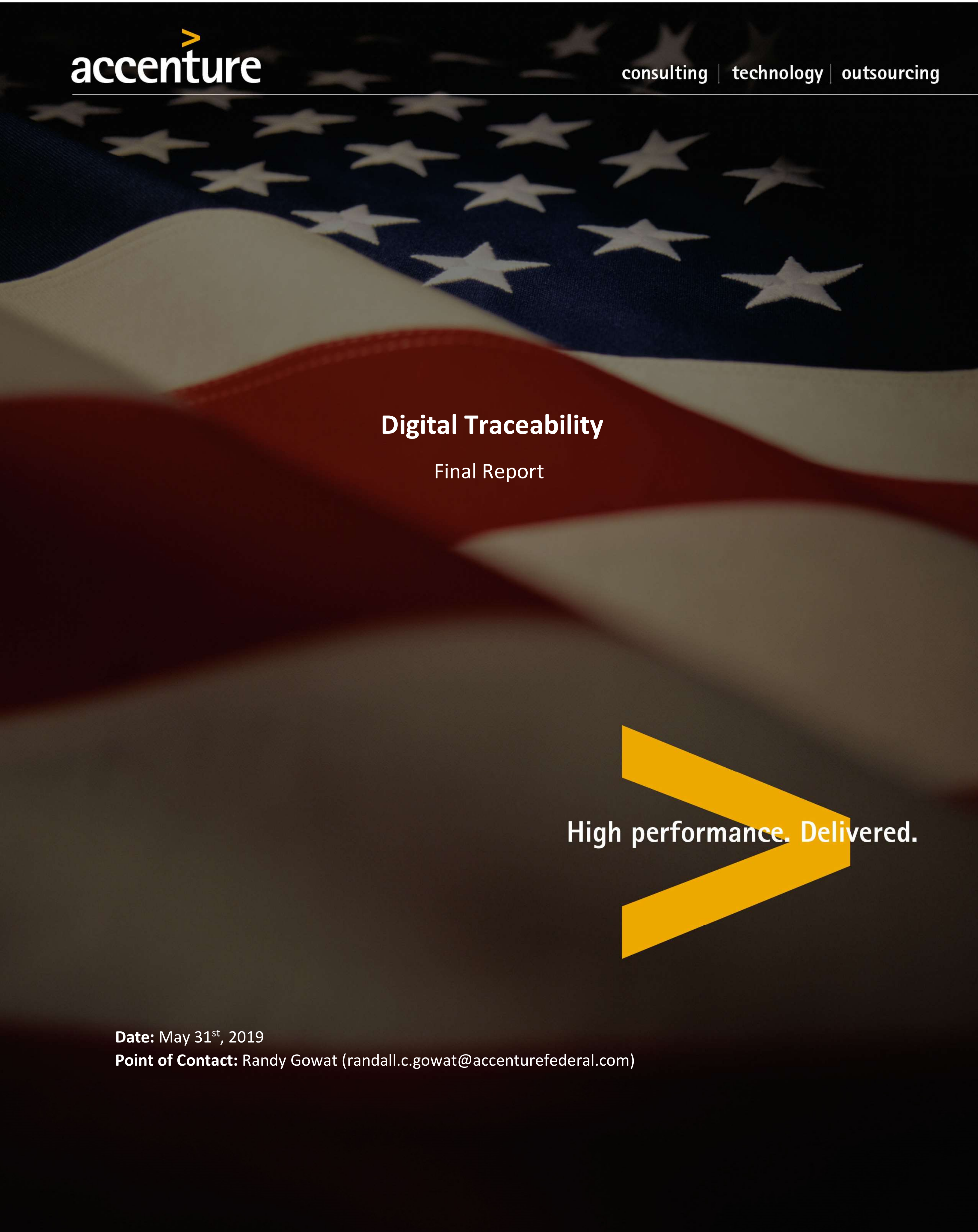
accenture

consulting | technology | outsourcing



Digital Traceability

Final Report

High performance. Delivered.

Date: May 31st, 2019

Point of Contact: Randy Gowat (randall.c.gowat@accenturefederal.com)

Table of Contents

List of Figures

List of Tables

Executive Summary

The Digital Traceability project began as an analysis of the Counterfeit Detection and Avoidance Program (CDAP), with the goal of recommending functional and technical requirements for modernizing and digitizing the program. Initial research into CDAP revealed that this key program was fettered with manual processes and external user submission errors leading to significant delays and re-work. The root cause of many of these delays was found to be the manual submission of a paper copy of Form-918, the document external users submit to DLA with relevant business information. More specifically, delays were being caused by external users (i.e. vendors) submitting incomplete paper forms, or forms with blatant errors (e.g. information written in incorrect fields) leading to more than half of all submissions being returned for correction.

Recommended enhancements were developed to digitize collection of requisite CDAP information and automate portions of the review process where appropriate. These enhancements were laid out in future state process maps and accompanied by recommended requirements for J6 to consider. A digital Form-918 was prototyped and user tested by CDAP resources to demonstrate the future state external user experience. Additionally, a capacity analysis was performed to understand existing bottlenecks in the CDAP process and estimate time savings to be gained across various CDAP stakeholder groups as a result of the recommended digitization. This analysis incorporated potential CDAP workload increases which are expected with the addition of other critical Federal Supply Classes (FSC) including 5961, 5962, 5963, 5998, and 5999.

The recommended enhancements for CDAP include enterprise data storage, enabling better use of user-submitted data and reporting. To further bolster program efficiency and transparency, business intelligence dashboard views and metrics were developed using the J6 enterprise visualization tool, Qlik Sense. The inclusion of new technical touchpoints along the CDAP process required new contingency plans be developed to account for potential downtime across a variety of scenarios. In preparation for any potential disruptions in these underlying systems, both program-specific and enterprise-wide contingency plans were documented.

In the course of recommending improved data collection procedures for CDAP, similar programs requiring manual data collection were discovered including Trade Security Control (TSC) and the Joint Certification Program (JCP). TSC controls the transfer of certain property outside of DoD control and JCP reviews requests to access export controlled technical data. Although both programs would benefit from the web-based data collection approach recommended for CDAP, the information collected in DD Form 1822 (TSC) and DD Form 2345 (JCP) exists at a higher sensitivity level, including personally identifiable information (PII). As such, the Digital Traceability project was extended to analyze these processes and recommend requirements for secure collection and transmission of this information. The subsequent analysis of these programs found that they too experience unacceptable user-submission error rates and highly manual processes. Recommendations for improving these processes via digitized web-form, automated validations, and enterprise data storage were documented and a proposed technical architecture diagram encompassing all three programs was created.

1.0 Introduction

DLA is the DoD’s supply source for nearly 85 percent of its spare parts and supports more than 2,430 weapon systems, including nearly all consumable items (fuel, food, construction material, etc.). With over 9,000 contracts processed daily to meet this vigorous demand, DLA is especially vulnerable to suppliers providing counterfeit, non-conforming, and malicious items.

In response to these risks, both the government and DLA have made Supply Chain Risk Management (SCRM) a priority. This is emphasized in the DLA 2018-2026 Strategic Plan, where addressing (Objective. 1.3) and mitigating risk (Objective. 5.4) are listed as major enterprise priorities. Specifically, the Plan outlines that DLA should “Strengthen risk management to ensure secure, agile, and resilient combat logistics support” with a goal of ensuring “readiness and lethality across the end-to-end supply chain,” by reducing risk in areas such as counterfeiting.

- Objective 1.3: *“Ensure readiness and lethality across the end-to-end supply chain by reducing risk, improving efficiency, and optimizing retail and industrial support…”*
- Objective 5.4: *“Strengthen risk management to ensure secure, agile and resilient combat logistics support…”*

CDAP is tasked with reviewing all awards for components in Federal Supply Class (FSC) 5962 to ensure vendors are properly qualified through vetting traceability and test report documentation. However, as DLA looks to expand this program to include additional supply classes in the future, CDAP resources are struggling to meet the growing traceability demand due to the highly manual and inefficient processes. This is particularly evident in the existing review process, which is manual and results in approximately 50 percent user submission error rate. As a result, this that requires vendors to repeat the traceability submission process as well as the traceability review itself. Each resubmission results in correspondence lag time, and the result is a traceability review backlog.

Another major issue with existing CDAP processes is that the database used to facilitate traceability review tracking is not integrated within DLA’s enterprise systems. Instead, the information is stored locally and exchanged between relevant participants in the DLA network. CDAP is crucial to mitigating the risk of potentially defective or malicious components from entering DLA’s supply chain, and therefore requires enhancements designed to streamline throughput and store the data within enterprise systems.

The Digital Traceability project aims to modernize existing CDAP processes by digitizing the collection, analysis, and storage of traceability documentation – including Form-918 and traceability/test report information. These Digital Traceability enhancements, including the recommend web-based data collection form, will provide built-in validations and reduce vendor submission errors. A web-based form will also automate data collection into enterprise systems, providing relevant DLA users with easy access to traceability and related data. Finally, the enhancement recommendations suggest that DLA utilize the enterprise visualization tool to create business intelligence dashboards for CDAP users. These dashboards will allow the CDAP team to understand expected review volume, easily track the status of each contract review, and provide ongoing trend analysis. Ultimately, the primary goals of these enhancements are to improve existing review processes and enable DLA to expand to other supply classes within the Counterfeit Detection and Avoidance Program without reaching capacity.

2.0 Counterfeit Detection and Avoidance Program (CDAP)

Reports published by the Department of Defense and Government Accountability Office (GAO) make the threat of counterfeit and nonconforming parts entering the DoD supply chain abundantly clear. These reports identify electronic components as major targets for malicious activities due to their abundance in critical systems and their ability to be maliciously programmed or otherwise compromised. In response to this increased threat, DLA has tasked its CDAP team to conduct an additional analysis and review prior to the acquisition of the highest-risk electronic components. Currently, the CDAP process and additional protections are applicable for every acquisition of FSC 5962 components (Electronic Microcircuits). Vendors who are awarded contracts in this FSC are required to meet certain levels of qualification and must provide material evidence of their qualification in the form of test reports or traceability documentation prior to shipping the materiel to DLA.

2.1 Counterfeit Detection and Avoidance Program (CDAP) Stakeholder Groups

The Counterfeit Detection and Avoidance Program relies on a high level of cross-team participation from multiple groups within DLA and some external partners. The following sections provide a brief description of each team and their role in the overall CDAP process.

2.1.1 CDAP Management & Review Team

The CDAP program is managed and operated by a team of J3 resources based out of DLA Land & Maritime. This team is responsible for communicating with vendors who have won awards within covered supply classes (only Federal Supply Class 5962 currently) to determine their qualification level and ultimately review and approve or reject supplemental documentation. This team is the primary Technical Quality group responsible for communication with external vendors and coordinates with other teams throughout the CDAP process to track procurements throughout their CDAP lifecycle.

2.1.2 Test Laboratory Team

The Test Laboratory team is responsible for inspecting electronic microcircuits received through the CDAP process and for applying appropriate markings if the components pass inspection. The Test Laboratory receives items that have passed the 'first look' from DDWO and performs x-ray inspections on all received components. Once a microcircuit has passed the x-ray inspection, it is marked with DNA provided through external partner Applied DNA Sciences and tracked within Test Laboratory databases.

2.1.3 Warehousing Team

The Warehousing team, sometimes referred to as 'DDWO' or 'Defense Distribution Warren Ohio', is the group that directly receives shipments of FSC 5962 components from vendors. This group, which is co-located with the Test Laboratory Team onsite, receives shipments and performs the 'quick look' process. The 'quick look' consists of comparing package contents with cover sheets and procurement information to ensure the items match what is expected and are packaged properly (in most cases, this means enclosure in static-resistant packaging). Once the warehousing team has determined that a shipment passes 'quick look', they move the items on to the Test Laboratory to continue the CDAP process.

2.1.4 Procurement Team

The Procurement Team bookends the CDAP process and plays a key role in both pre-award and post-award phases. Pre-award, the Procurement team collaborates with CDAP Management to ensure that winning bidders are eligible for award. After awarding a Purchase Order, the procurement team does not participate in the process (aside from general awareness/tracking) until any post-award actions are required.

2.2 Counterfeit Detection and Avoidance Program (CDAP) Processes

2.2.1 Pre-Award Qualification

Vendors must obtain a level of trusted qualification with DLA before being eligible to complete the requirements of an FSC 5962 award and deliver the materiel to DLA. It is unclear whether a vendor's qualification status is considered by contracting officers during the solicitation bid review process, but lack of any qualification will ultimately be a disqualifying factor if the awarded vendor cannot properly certify their merits with the CDAP team. There are five types of qualifications which would allow a vendor to participate in an FSC 5962 acquisition including:

(1) **Approved Source Manufacturer Specified in the Solicitation/Contract Item Description (Original Component Manufacturer (OCM), Original Equipment Manufacturer (OEM))** – the source identified by name, Commercial and Government Entity (CAGE) code, and part number listed in the purchase item description in Section B of the award. This entity only qualifies as OCM/OEM if they are the original manufacturer of the part, the original component manufacturer, the original equipment manufacturer, the manufacturer specified in the solicitation/contract item description, or the part Design Control Activity (DCA), which is defined as the entity having responsibility for the design of a given part and for the preparation and currency of engineering drawings and other technical data (TD) for that part.

(2) **Approved Source on the Applicable Qualified Products List (QPL)/Qualified Manufacturers List (QML) –** requires a Certificate of Conformance and Traceability (CoC/T) and must include information and documentation required by the applicable military specification for the QPL/QML product, that is listed on the DLA Technical and Quality Requirement RQ007**.**

(3) **Authorized Distributor of the OCM/OEM or QPL/QML Approved Source** – A supplier who has a contractual arrangement or the express written authority with the OCM/OEM of the item being acquired to buy, stock, re-package, sell, and distribute the item specified in the solicitation/contract.

(4) **Supplier/Distributor on the Qualified Supplier List of Distributors (QSLD) for FSC 5961/5962** – A distributor listed or determined qualified for listing on the DLA Land and Maritime Qualified Supplier List of Distributors for FSC 5961/5962.

(5) **Supplier/Distributor on the Qualified Testing Suppliers List (QTSL) for FSC 5961/5962 –** A distributor listed or determined qualified for listing on the DLA Land and Maritime Qualified Testing Suppliers List (QTSL) for FSC 5961 and 5962.

2.2.2 Award and Certification of Qualification

Once a vendor has been awarded a contract to provide an FSC 5962 part, they must provide the CDAP office with proof, or certification, of their qualification in one of the five previously described qualification levels. This process must be completed at least fifteen days prior to the delivery date specified in the contract and requires a minimum of two documents be sent in for CDAP review: (1) a Traceability / Test Documentation Cover Sheet (also known as DLA Land and Maritime Form-918) and (2) Traceability proof or Test Report documentation. Information pertaining to the required documentation and a link to Form-918 are located on the DLA Land and Maritime CDAP webpage (http://www.dla.mil/LandandMaritime/Business/Selling/Counterfeit-Detection-Avoidance-Program/). The Traceability / Test Documentation Cover Sheet (Form-918) is always required, but the other documentation depends on the level of qualification met by the vendor. In general, the most qualified vendors (typically OCM/OEMs) require the least additional documentation while the least qualified vendors require more robust documentation for the traceability review. The traceability/test documentation requirements as listed on Form-918 are described below.

Traceability/Test Documentation Requirements in Accordance with DFARS 252.246-7008 & DLAD Procurement Note M01 Approved Suppliers for FSC 5961 Semiconductors and FSC 5962 Electronic Microcircuits:

(1) **Approved Source Manufacturer Specified in the Solicitation/Contract Item Description (Original Component Manufacturer (OCM), Original Equipment Manufacturer (OEM))** – Completed DLA L&M Form-918. If the bare item markings on the parts being provided do not match the CAGE and part number specified in the item description in the contract, the supplier must provide documentation certifying that the parts containing the alternate markings are the "exact product" as the item represented by the CAGE and part number specified in the contract item description.

(2) **Approved Source on the Applicable Qualified Products List (QPL)/Qualified Manufacturers List (QML)** – Completed DLA L&M Form-918. Also requires a Certificate of Conformance and Traceability (CoC/T), which must include information and documentation required by the applicable military specification for the QPL/QML product. Refer to DLA Technical and Quality Requirement RQ007.

(3) **Authorized Distributor of the OCM/OEM or QPL/QML Approved Source** – Completed DLA L&M Form-918 and evidence of a contractual arrangement with or the express written authority of the manufacturer or current design activity to buy, stock, sell, or distribute the part and an unbroken chain of traceability documentation through authorized distributors (if applicable), back to the approved source/manufacturer specified in the solicitation/contract.

(4) **Supplier/Distributor on the Qualified Supplier List of Distributors (QSLD) for FSC 5961/5962** – Completed DLA L&M Form-918 and evidence of an unbroken chain of traceability documentation, through trusted providers, back to an approved manufacturer specified in the solicitation/contract item description. Refer to the QSLD-5961/5962 document. QPL/QML items require a Certificate of Conformance and Traceability (CoC/T), which must include information and documentation required by the applicable military specification for the QPL/QML product. Refer to DLA Technical and Quality Requirement RQ007.

(5) **Supplier/Distributor on the Qualified Testing Suppliers List (QTSL) for FSC 5961/5962** – Completed DLA L&M Form-918 and complete test report including summary of test results, electrical testing read and record data, device photos, etc. Traceability documentation to the source of parts provided for testing. Refer to DLAD Procurement Note M01.

As previously described, the completed Form-918 and other documentation (as required) must be sent to the CDAP office at least fifteen days prior to the contract delivery date (CDD) via fax or email. This requirement allows the CDAP team sufficient time to review the documentation and provide approval or rejection notices as applicable. In the case where Form-918 has any errors, the CDAP team will notify the vendor and require resubmission of the documents. If Form-918 errors persist through more than two or three resubmissions the order is often cancelled.

If there are any discrepancies between the product number listed on the award and the product number provided by the vendor on Form-918, the CDAP team will first escalate the issue to a DLA Product Specialist or the appropriate Military Service Product Specialist before notifying the vendor. The Product Specialist will assess if the proposed substitute product is acceptable in lieu of the original requested part. If so, the alternate product number will be accepted, otherwise the substitute product will be rejected, and the order will be cancelled.

If all the information provided within Form-918 is acceptable, the CDAP team will review any additional documentation including test reports, traceability documentation, etc. This may include validating the chain of custody through traceability documentation, certification of the test report results, or other validation approaches. Once it has been determined that all submitted documentation is valid, the CDAP team will provide approval by signing Form-918 and sending it along with a ship letter to the vendor. This process also typically includes internal processes such as manually entering the Form-918 data into the CDAP catalog and uploading the documentation to Records Management (RM) within the Enterprise Business Systems (EBS).

2.2.3 Vendor Shipment

Upon receipt of a signed Form-918 from the CDAP team and approval to ship letter, the vendor is then able to complete the delivery process. The vendor must ship the materiel to the receiving warehouse co-located with CDAP at DLA Land & Maritime – Defense Depot Warren Ohio (DDWO) along with copies of all aforesaid required documentation – the signed Form-918, approval to ship letter, and any other required traceability documentation and/or test reports. These hard copies of documentation are required as further validation of the items throughout the CDAP process.

2.2.4 DDWO Receiving and Quick Look

When the shipped items and hard copies of required CDAP documentation are received at DDWO, the warehouse resources perform a process called a ‘quick look’. This process involves comparing the information contained within the documentation to the parts themselves and the information entered in the CDAP catalog. If any information or product discrepancies are identified, a Supply Discrepancy Report (SDR) is generated. If the discrepancy is minor, the vendor is notified of a need to modify the order and resubmit all required documentation, otherwise the order is cancelled.

However, if all provided information is valid and matches the items provided, the ‘quick look’ passes and is sent on to the test laboratory, which is also co-located at DLA Land & Maritime.

2.2.5 Test Laboratory Process

Once an FSC 5962 item is received at the test laboratory, the laboratory team performs a visual and x-ray inspection according to industry standards. If an item does not pass the visual inspection it is deemed unacceptable and the order is cancelled. If the part has significant defects or is suspected to be a potential counterfeit, the case is also sent for a legal review. However, if the item passes the visual inspection, it is put through a deoxyribonucleic acid (DNA) marking process to help track the parts throughout the DoD supply chain. This DNA marking program is administered by the test lab and in conjunction with a DLA third party partner, Applied DNA Sciences (ADNAS).

2.2.6 Final Approval and Inventory

Once an item has passed a visual inspection and marked with DNA, it is deemed genuine the information for this contract is updated within RM to indicate the process has completed. The materiel is then passed back to DLA Procurement (J7) so that it could be added to the overall inventory and is eligible to be shipped to DLA customers.

2.3 Inefficiencies within Existing CDAP Processes

The existing CDAP processes, as described in sections 2.2.1 through 2.2.6, are manually intensive and prone to inefficiencies. Through stakeholder engagement and working sessions to analyze these processes, several areas for improvement were identified. These issues with the existing CDAP processes have a variety of causes and impact DLA stakeholders throughout the entire review, delivery, and receipt processes.

MANY MANUAL PROCESSES
DATA SUBMISSION PRONE TO ERRORS
LACK OF VISIBILITY DURING REVIEW
NO ENTERPRISE INTEGRATION

Figure 1. *Summary of Issues with Existing CDAP Traceability Review Process*

2.3.1 Many Manual Processes

Once an FSC 5962 award has been made, the subsequent steps required to collect, validate, and save vendor information are all manually labor-intensive activities. These steps include a review of the actual vendor-submitted information, a comparison to ensure the data matches submitted traceability information, and a validation of qualification levels – for both the submitting vendor and any Original Equipment Manufacturer / Original Component Manufacturer (if applicable). Not only are these steps currently performed manually, but they are prone to error as a result.

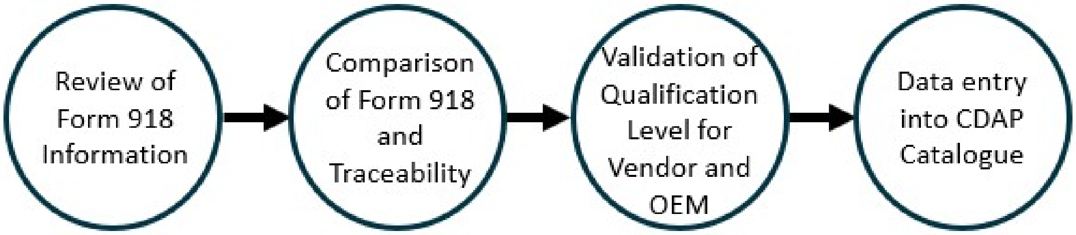

Review of Form 918 Information
Comparison of Form 918 and Traceability
Validation of Qualification Level for Vendor and OEM
Data entry into CDAP Catalogue

Figure 2. *Progression of Manual Traceability Review*

2.3.2 Vendor Data Submission Prone to Error

The current CDAP traceability submission process requires vendors who have been awarded an FSC 5962 contract to provide traceability documentation along with a Traceability/Test Documentation Cover Sheet, also known as the DLA Land & Maritime Form-918. This form collects basic information about the vendor, details of the original part manufacturer, and certification of the vendor's qualification, among other pieces of information. This entire form is currently filled out and sent to the CDAP team as either a physical hard copy or completed as a Portable Document Format (PDF) file.

Due to the free-form nature of this process, vendors often put information within the wrong fields or fill out the form incorrectly, resulting in approximately half of all CDAP submissions containing errors. This high error rate continues to drive re-work on behalf of both the vendor and the CDAP team. When errors are found on Form-918, the CDAP team must notify the vendor to make corrections, which requires a both correspondence with the vendor as well as them resubmitting the form. For each resubmission another review is required, creating redundant work for the CDAP team. In cases where errors persist beyond three reviews, the CDAP team must terminate the contract, which often leads to backorders and a new procurement process to be triggered.

2.3.3 Lack of Visibility During Review Process

The actions required to move an acquisition through the CDAP process and into DLA's inventory requires participation from several groups internal to DLA. These groups include the Technical Quality (TQ) team, the DDWO receiving team, the Test Lab team, and the Procurement team. Although the process of fully acquiring new FSC 5962 components involves actions and interdependencies among all these teams, there is a lack of visibility among teams until their specific actions is triggered or completed. For example, a vendor may submit traceability information along with their Form-918 basic data, but the DDWO receiving team may not know that the vendor is close to providing a delivery until the CDAP team confirms traceability, sends back an 'approval to ship' notice, and updates the shared data and progress record – the CDAP Catalog.

2.3.4 Lack of Enterprise Integration

The record of procurements and progress for the entire CDAP process, called the CDAP Catalog, is stored locally and shared among DLA stakeholder groups. This database houses information about specific contracts and actions that have been taken; yet is only updated when major steps are completed, and the database is refreshed.

The local storage and sharing of the CDAP Catalog has a negative impact on the usability and future application of data collected during the review process. Without a method for connecting this information to enterprise systems, or sharing information in real-time with disparate stakeholder groups, the data has a lessened impact. Additionally, the lack of an enterprise data storage solution reduces the auditability of the information and potential use or analysis for related efforts. This lack of integration also prevents the CDAP team from utilizing procurement business systems to easily cross-check submitted information, instead requiring a resource to manually review each field.

3.0 CDAP Capacity Analysis

The primary goal of existing CDAP processes is to ensure vendors providing high-risk components are effectively qualified to provide such components, prior to DLA receiving shipments of such materiel. The Counterfeit Detection and Avoidance Program plays an important role in protecting DLA against potential fraud by providing an additional level of due diligence and qualification for some of the enterprise's most at-risk components. Based on recent Office of the Secretary of Defense (OSD) guidance and Supply Chain Risk Management (SCRM) policies, there has been an increased interest in expanding the coverage of CDAP to additional part classes, beyond the existing review of FSC 5962. In addition to current CDAP coverage for FSC 5962 (Electronic Microcircuits), it has been proposed that the following component classes also be considered:

- **FSC 5961** - Semiconductor Devices and Associated Hardware
- **FSC 5963** – Electronic Modules
- **FSC 5998** - Electrical and Electronic Assemblies, Boards, Cards, and Associated Hardware
- **FSC 5999** - Miscellaneous Electrical and Electronic Components

While an expansion of the program to other part classes would allow DLA to more effectively manage the risk of potential fraud, such an expansion would also necessitate an increased workload for CDAP resources. However, CDAP management has noted that current resources are already working at their maximum capacity to maintain existing review levels. As such, an analysis of the capacity of the CDAP program was proposed to assess current review capacity and the expected capacity with recommended enhancements in place. This assessment will provide DLA HQ and CDAP leadership with a better understanding of the resource workload requirements across participant teams needed to handle the throughput expected from each FSC listed above.

3.1 Methodology

The objectives for analyzing CDAPs workload capacity were (1) assess the existing capacity of CDAP reviewing FSC 5962, (2) analyze the DLA identified FSCs to potentially be added to CDAP, and (3) determining the impact of expanding CDAP to additional FSCs. The scope of the review included all CDAP stakeholders and their respective processes.

The existing capacity of CDAP was determined by analyzing the existing processes of CDAP stakeholders through client interviews and site visit discovery. The findings were documented in process maps and used to identify process improvement opportunities. Key DLA stakeholders collaborated in the development of the current and future state process designs. The CDAP Catalog was used to develop an understanding of the award lifecycle and volumes for FSC 5962. A benchmark CDAP model reflecting the existing state capacity was developed through these findings.

The second objective was addressed by analyzing J6 procurement data to gather information on award volumes and trends of the FSCs identified by DLA. The existing state model was then adjusted to reflect a future state with process improvements and extrapolated to the other FSCs.

Lastly, the benchmark model was used to compare to the outcomes of the future state model. The analysis of the future state model determined the impact to workload and Full Time Equivalent (FTE) requirements for an expanded CDAP.

3.1.1 General Capacity Model Framework

A workload capacity model is used to determine the capacity of a process and predict the impact to changes to the process. A standard three phase approach was used to frame the development of the model and analysis, as shown in Figure 3.

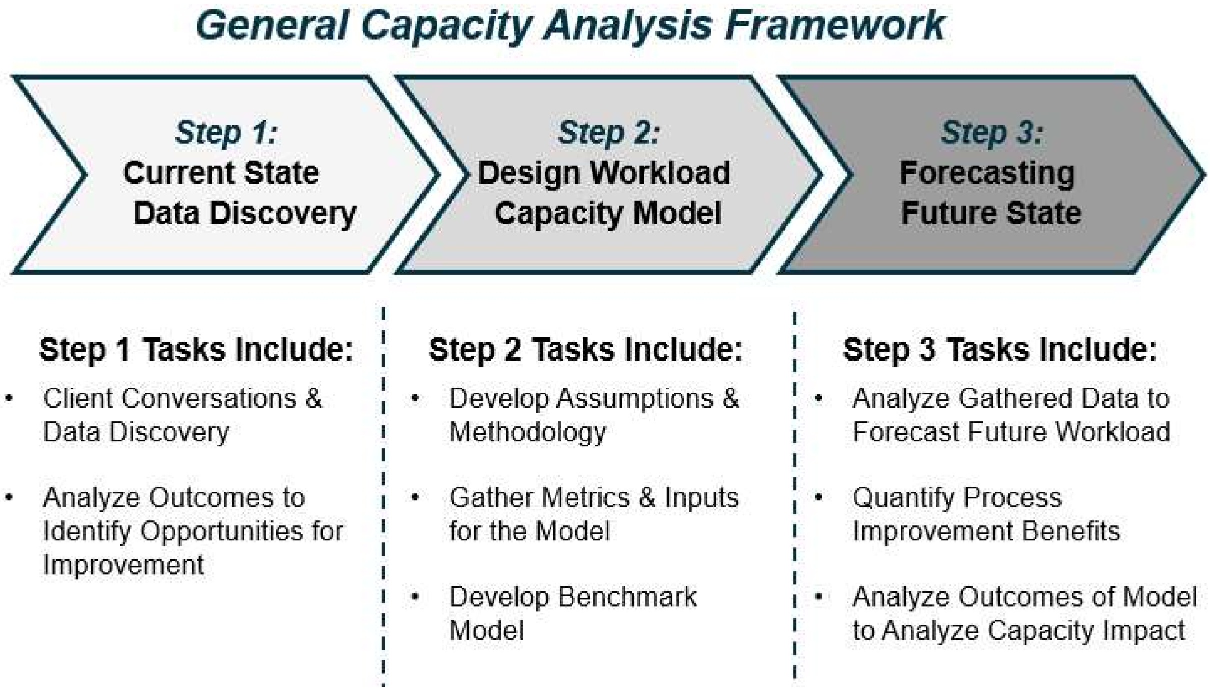

General Capacity Analysis Framework
Step 1: Current State Data Discovery
Step 2: Design Workload Capacity Model
Step 3: Forecasting Future State
Step 1 Tasks Include:
• Client Conversations & Data Discovery
• Analyze Outcomes to Identify Opportunities for Improvement
Step 2 Tasks Include:
• Develop Assumptions & Methodology
• Gather Metrics & Inputs for the Model
• Develop Benchmark Model
Step 3 Tasks Include:
• Analyze Gathered Data to Forecast Future Workload
• Quantify Process Improvement Benefits
• Analyze Outcomes of Model to Analyze Capacity Impact

Figure 3. *General Capacity Analysis Framework*

3.1.1.1 Current State Data Discovery

The current state data discovery phase is used to gain a holistic understanding of the businesses processes and the roles and responsibilities of employees. The findings are documented in process maps to outline workflow. Lastly, in this phase the documented processes can be analyzed to identify pain points and opportunities for improvement.

3.1.1.2 Design Workload Capacity Model

The second step is designing the workload capacity model specifically for the process being analyzed and designed to predict the impacts to the business. Once the methodology and assumptions have been outlined, the existing state of the process is replicated as a benchmark. A benchmark is used to reinforce the accuracy of the model, if the existing state cannot be replicated then the model will do little to predict the future impacts to the business. The benchmark model should represent the existing state of the business process, such as process times, existing employee structure, and the existing levels of capacity.

3.1.1.3 Forecasting Future State

The third step is focused on the future impacts to the business process. In this step, metrics needed to replicate the changes to the business process are gathered through further client discussions and site visit discoveries. Any identified improvements to the processes found during step 1 should be quantified to be inputted into the model. The outcomes of the model are analyzed and used to make data driven business decisions.

3.1.2 CDAP Capacity Model Framework

The CDAP Capacity Model was developed to analyze the impact of potentially adding additional FSCs to the CDAP process. The approach outlined in the previous section was used to guide the design and development of the CDAP Capacity Model.

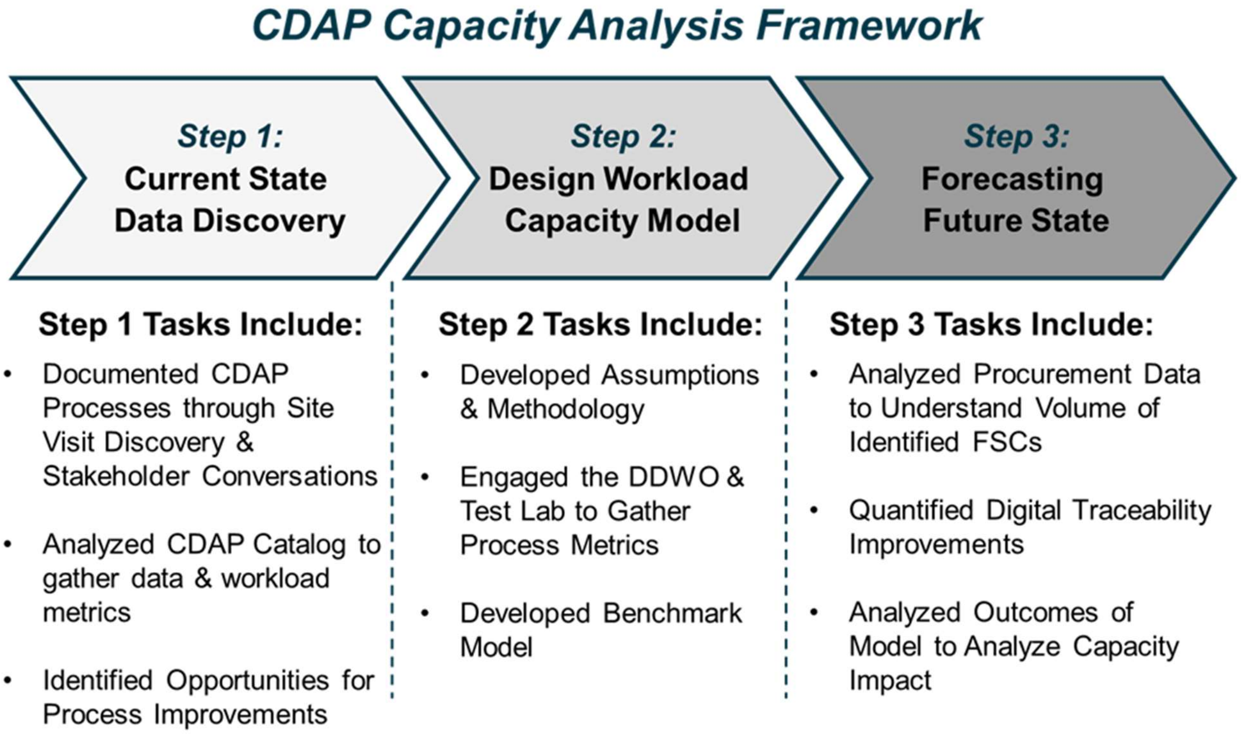

CDAP Capacity Analysis Framework
Step 1: Current State Data Discovery
Step 2: Design Workload Capacity Model
Step 3: Forecasting Future State
Step 1 Tasks Include:
• Documented CDAP Processes through Site Visit Discovery & Stakeholder Conversations
• Analyzed CDAP Catalog to gather data & workload metrics
• Identified Opportunities for Process Improvements
Step 2 Tasks Include:
• Developed Assumptions & Methodology
• Engaged the DDWO & Test Lab to Gather Process Metrics
• Developed Benchmark Model
Step 3 Tasks Include:
• Analyzed Procurement Data to Understand Volume of Identified FSCs
• Quantified Digital Traceability Improvements
• Analyzed Outcomes of Model to Analyze Capacity Impact

Figure 4. *CDAP Capacity Model Framework*

3.1.2.1 Analyzing Existing State of CDAP

In the initial phase of the Digital Traceability effort, conversations were held with CDAP stakeholders to understand the existing processes of CDAPs traceability review. The findings were documented in current state process maps. Once the processes were initially documented, a collaborative and iterative approach with CDAP stakeholders was used to ensure accuracy. The process maps were then analyzed and opportunities for improvement were identified as the 'Digital Traceability' enhancements as mentioned in previous sections of this report.

3.1.2.2 Developing a CDAP Capacity Model

In step two, a methodology was used to design the model to analyze the impact of additional FSCs to the CDAP traceability program. The approach consists of two parts, analyzing the impact of additional FSCs under existing CDAP processes, and analyzing the impact of additional FSCs to an enhanced CDAP process. Step two of the capacity model approach focuses on replicating the existing state of the CDAP process in the model. This is used as a benchmark to compare the outputs of the model and to ensure accuracy. Before replicating the existing state, the entire CDAP process needed to be captured in the model. Other stakeholders such as the Test Lab and DDWO at Land & Maritime were engaged in similar activities as mentioned in step 1. The processes of the Test Lab and DDWO were mapped in process maps and analyzed to identify opportunities for improvement. During this engagement, inputs for the benchmark are gathered such as process times, roles and responsibilities of available resources, and volume metrics from the CDAP Catalog. The benchmark model was confirmed and accepted by CDAP stakeholders as accurately representing the existing state.

3.1.2.3 Analyzing Impact of CDAP Expansion

Forecasting the future state and outputting the impact to FTEs required for the expanded CDAP process is the goal of step three. DLAs procurement data was used to understand the volumes of the identified FSCs. The impact of the Digital Traceability enhancements were quantified to represent an enhanced future state of CDAP. The results of the model represent an expanded CDAP under two future state conditions; an error-free (clean) state and error state. The required FTEs are predicted by the model for both states and can be further analyzed to understand how CDAP can expand its review process to other high-risk FSCs.

3.2 CDAP Current State Capacity Analysis

The existing state of CDAP was replicated in a model to determine CDAPs existing capacity reviewing FSC 5962. Data was gathered through client interviews, site visits, CDAP data, and DLA procurement data. The findings from this analysis led to the development of current and future state process maps, identified opportunities for improvement, and a benchmark model that reflects CDAPs existing capacity.

3.2.1 Current State Assumptions

Developing a workload capacity model requires certain assumptions to account for unknowns and provide structure to the model. Employee productivity assumptions were made using data provided by the Office of Personnel Management (OPM). The CDAP Catalog and J6 Procurement data were used to analyze award volumes. The assumptions for the current state assessment are described in the following sections.

3.2.1.1 Determining FTE Capacity

A calculation for the workload capacity of one employee during a year is crucial for determining not just the current state of the traceability review workload, but also how capacity would increase with the implementation of a digital Form-918. Estimates of how capacity and efficiency would be affected through a digital Form-918 yielded results of a large overall increase. These efficiency gains and their rationale will be discussed in greater detail in subsequent sections.

In collaboration with the CDAP stakeholders, each step in the traceability review process was analyzed and discussed to quantify the effort needed to complete tasks. Key metrics such as error rates of submissions, communication delays, and other process nuances were discussed and quantified.

The work capacity for one employee during a year is calculated and is based on the total amount of workdays per year while accounting for deductions such as federal holidays, paid leave, training, and overhead. The factors taken into consideration for calculation of FTE capacity are detailed as follows.

Table 1. *Productivity Estimates*

Factor	Days
Workdays per Year	260
Federal Holidays	-10
Time Unavailable Due to Illness/Vacation	-33
Training	-5
Overhead	-5
Total Available Days	**207**
Sub-Total Hours	**1,656**

A total of 1,656 hours are estimated for each FTE reviewing traceability. While this number is backed by up-to-date information available from OPM and other government agencies, it should be taken with interpreted with a small margin of error due to any unforeseen events. For the purpose of the capacity model, this margin of error is ignored, and it is assumed each resource will use all of their respective time off in a given year.

3.2.1.2 Data Assumptions

The CDAP Catalog and J6 Procurement data were the data sets used to determine the award lifecycle and the volume of awards. The CDAP Catalog gave insight into FSC 5962 volumes, and the lifecycle of an award in the CDAP process. J6 Procurement data was used to analyze the volumes of the identified FSCs and respective trends. The current state analysis and findings were reviewed and confirmed by CDAP stakeholders, which guides the development of the estimated process times. These process times and the relying data are assumed to be accurate based on client acceptance.

The data assumptions used to guide the CDAP workforce capacity model were the following:

- The volume of awards for each respective FSC will be similar to historical volumes
- The processes to review the traceability of FSCs other than 5962 will be similar
- Form 918 and the data it collects will be the same for FSCs other than 5962
- Auto-awards of the identified FSCs will be converted to manual awards if added to CDAP
- J6 Procurement Data was queried accurately and to the requested specifications
- CDAP Catalog data has been reconciled and up to date in accuracy

3.2.2 Analysis of Current State Processes

The current state processes were analyzed and documented through client site visits, client interviews, and collaborative working sessions to develop an understanding of CDAP processes. This analysis produced process maps of each stakeholders' processes. The process maps were used to identify each task and step in the CDAP process and mapped to respective process times. These estimates were confirmed with CDAP stakeholders to ensure the accuracy of the model.

3.2.2.1 CDAP Management Process

The CDAP management process is specifically the initial traceability review team who is tasked with the first chain of custody review and ultimately tasked with approving or denying FSC 5962 awards. The current state CDAP process map is shown on the next page to guide the process times discussion.

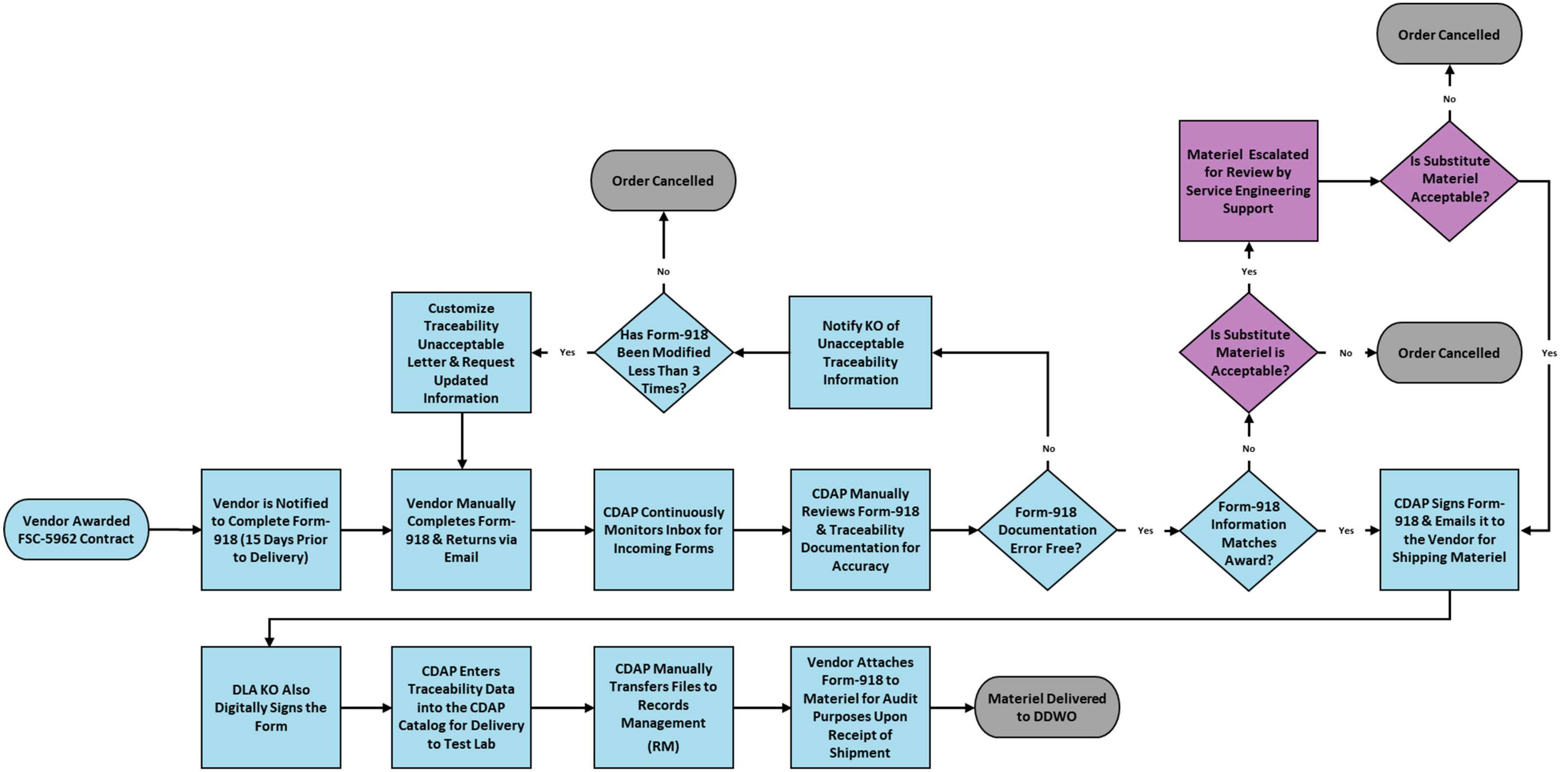

Order Cancelled
No
Materiel Escalated for Review by Service Engineering Support
Is Substitute Materiel Acceptable?
Order Cancelled
No
Yes
Customize Traceability Unacceptable Letter & Request Updated Information
Yes
Has Form-918 Been Modified Less Than 3 Times?
Notify KO of Unacceptable Traceability Information
Is Substitute Materiel is Acceptable?
No
Order Cancelled
Yes
No
No
Vendor Awarded FSC-5962 Contract
Vendor is Notified to Complete Form-918 (15 Days Prior to Delivery)
Vendor Manually Completes Form-918 & Returns via Email
CDAP Continuously Monitors Inbox for Incoming Forms
CDAP Manually Reviews Form-918 & Traceability Documentation for Accuracy
Form-918 Documentation Error Free?
Yes
Form-918 Information Matches Award?
Yes
CDAP Signs Form-918 & Emails it to the Vendor for Shipping Materiel
DLA KO Also Digitally Signs the Form
CDAP Enters Traceability Data into the CDAP Catalog for Delivery to Test Lab
CDAP Manually Transfers Files to Records Management (RM)
Vendor Attaches Form-918 to Materiel for Audit Purposes Upon Receipt of Shipment
Materiel Delivered to DDWO

Figure 5. *Current State CDAP Process Map*

The total amount of time required for a CDAP resource to complete the traceability review of a FSC 5962 award without submission errors, is approximately 49 minutes. This consists of an estimated 30 minutes to review Form-918 and traceability documentation. The 'Sign & Send Shipment Notification' is estimated to take approximately 7 minutes, consisting of resources gathering signatures of approval and mailing documentation to the vendor. The existing process requires CDAP resources to manually enter information into the CDAP Catalog and manually upload it into Records Management (RM). This estimated time of approximately 12 minutes assumes CDAP resources are not making mistakes when entering data into the CDAP Catalog.

Table 2. *Existing CDAP Process Times*

CDAP - Current State Tasks	**Clean State**	**Error State**
Review Traceability	30	60
Communication with Vendor	3	10
Product Specialist	0	3
Upload Data to CDAP Catalog	10	10
Sign & Send Shipment Notification	7	7
Total Time (minutes)	**50**	**90**

The most significant impact to CDAPs capacity constraint is the current error rate of vendor submissions; approximately 50% of Form-918 documents contain trivial errors that require resubmission. The workload capacity model must account for these errors when estimating workload. Table 2 represents the CDAP tasks required when an error is present, and their respective estimated times. The reviewing of traceability documentation increases by 100%, due to the additional research required to verify the chain of custody. CDAP resources must access many different sources of information and perform ad-hoc research to confirm the validity of distributors claims. The substitute material task is specific to documentations with errors. This is due to a substitute product being proposed, which initiates a chain of tasks that require a product specialist to either approve or deny the proposed substitute component. The product specialist can take up to approximately 180 days to review the components, it is assumed that resources will work on other awards during the process specialist's assessment. The other tasks are not impacted by errors and assume the same estimated times as the 'no-error' state.

3.2.2.2 DDWO Process

In the existing process, the DDWO at DLA L&M receives vendors shipments and accompanying documentation. The quick look consists of comparing the shipment to the specifications in Form-918, and ensuring the components are packaged correctly. Aside from proper packaging, the DDWO does not need to review traceability, instead the components are moved to the product test lab for additional review and product testing. The total time of DDWO processes is estimated at approximately 20 minutes based on the three following steps: (1) Quick Look, (2) Entering Information into the Quality Information Database (QUID), and (3) sending the materiel to the Test Lab. The DDWO process can also be constrained by errors made by the vendor. For example, vendors shipping components to Land & Maritime that does not meet the required packaging specifications. Errors such as incorrect packaging require DDWO resources to generate a supply discrepancy report (SDR). The time to complete an award with errors is approximately 40 minutes due to discrepancies that arise during the quick look and the time to generate an SDR.

Table 3. *Existing DDWO Process Times*

DWWO - Current State Tasks	Clean State	Error State
Quick Look	10	20
Generate SDR Notification	0	5
Enter Information into QUID	5	10
Send Materiel to Test Lab	5	5
Total Time (minutes)	**20**	**40**

The process map shown in Figure 6, maps the DDWO and Test Lab processes on a single process map. The steps described in this section, and the subsequent Test Lab Process section are guided by the process map.

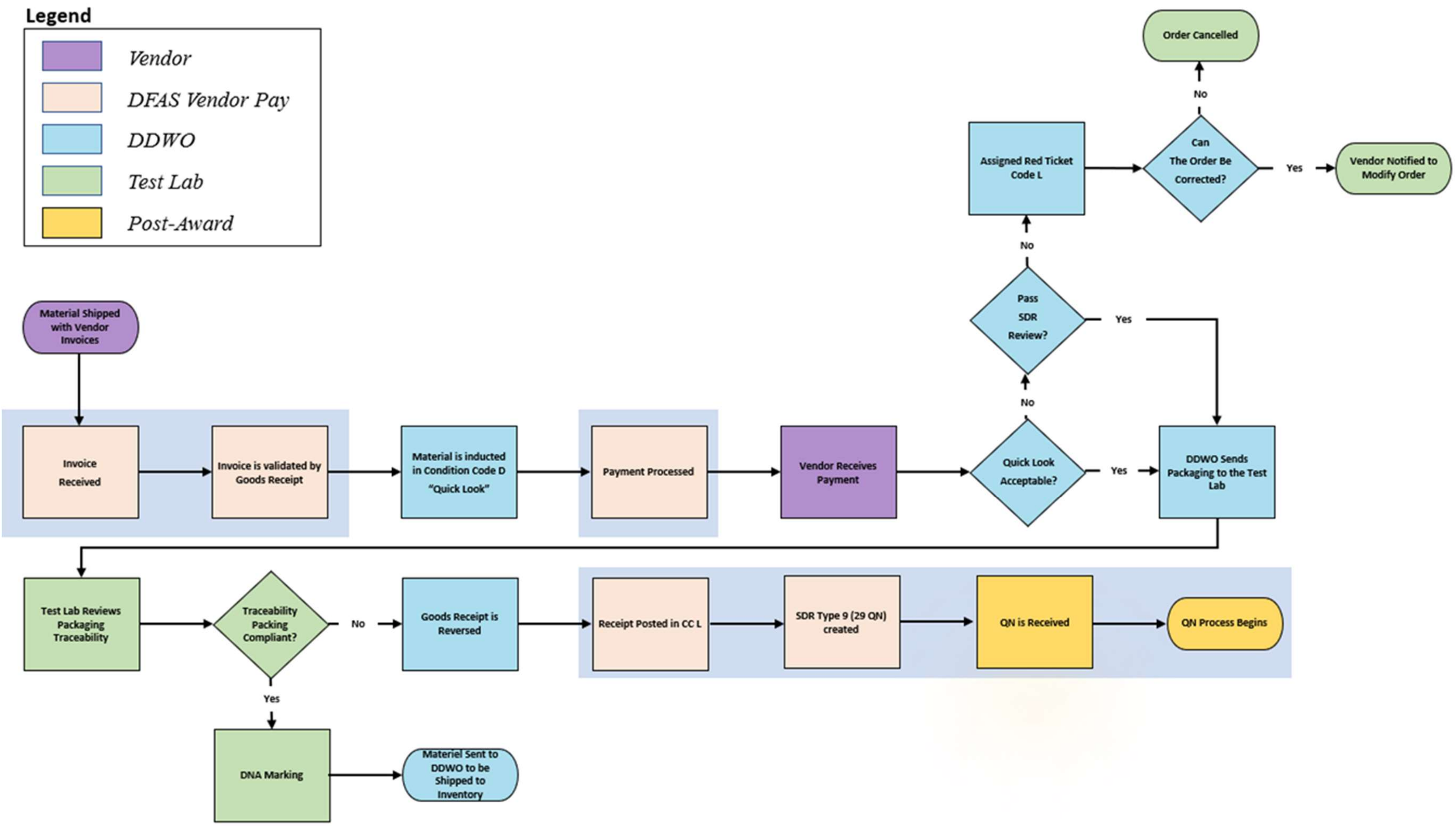

Legend
Vendor
DFAS Vendor Pay
DDWO
Test Lab
Post-Award
Material Shipped with Vendor Invoices
Invoice Received
Invoice is validated by Goods Receipt
Material is inducted in Condition Code D "Quick Look"
Payment Processed
Vendor Receives Payment
Quick Look Acceptable?
No
Yes
Pass SDR Review?
No
Yes
Assigned Red Ticket Code L
Can The Order Be Corrected?
No
Order Cancelled
Yes
Vendor Notified to Modify Order
DDWO Sends Packaging to the Test Lab
Test Lab Reviews Packaging Traceability
Traceability Packing Compliant?
No
Yes
Goods Receipt is Reversed
Receipt Posted in CC L
SDR Type 9 (29 QN) created
QN is Received
QN Process Begins
DNA Marking
Materiel Sent to DDWO to be Shipped to Inventory

Figure 6. *DDWO & Test Lab Current State Process Map*

3.2.2.3 Test Lab Process

The Test Lab at DLA L&M is responsible for conducting a second review of the documentation provided by vendors, testing components, and applying a unique DNA mark to each component. Due to the additional review needed, the Test Lab processes can take significantly longer if errors are present. In a state without errors the total time of Test Lab processes is approximately 75 minutes. Through site visit discovery, and discussions with Test Lab stakeholders each sub-process times were estimated. When the Test Lab receives the components from the DDWO, resources must unpackage the components to ensure they are the correct components purchased, not counterfeit products. In addition, a Test Lab resource must review the traceability documentation and verify its chain of custody, without errors, this takes approximately 10 minutes. DNA marking consists of marking each component with a DNA mark to ensure they are the correct components as they flow through the supply chain. The Test Lab has four DNA marking stations, of which they use only one or two stations depending on the quantity of components needing marking. After the parts are marked, they must be baked to seal the DNA marking. The Test Lab has two options when baking components – (1) traditional baking oven that takes about 60 minutes to complete, and (2) Ultraviolet (UV) baking which takes a significantly shorter amount of time but takes a larger effort to clean and maintain. Thus, traditional baking is used more often than UV baking. It is assumed that Test Lab resources are taking an estimated approximately 5 minutes to prepare for baking, then continuing to work on other tasks until baking is complete. Therefore, the model does not fully incorporate the 60 minutes it takes to bake components into the overall process time.

In a state with documentation errors, the most significant impact to the estimated process times is the time to review the traceability documentation provided by the vendor. Based on anecdotal findings from Test Lab stakeholders, the time to review a document with errors can take almost approximately 60 minutes compared to the approximately 10 minutes in the ‘clean’ state. Test Lab resources must perform ad-hoc research and reach out to CDAP resources to confirm any discrepancies. Once the documentation has been validated, the following processes are unaffected and have the same estimated process times. The increased time to review documentations with errors results in an increased Test Lab process time to approximately 120 minutes.

Table 4. *Test Lab Tasks*

Test Lab - Current State Tasks	**Clean State**	**Error State**
Unpackage Materiel	10	10
Review Traceability Documentation	10	55
Enter Data into QUID	5	5
X-Ray	10	10
DNA Marking	20	20
Baking Components	5	5
Repackage Materiel	10	10
Send Materiel to Depot	5	5
Total Time (minutes)	**75**	**120**

3.2.3 Data Analysis

The existing state of CDAP only conducts traceability reviews for FSC 5962. Using historical data from both the CDAP Catalog and procurement data, the estimated volume of awards can be seen in Figure 7. The average volume of FSC 5962 is approximately 1,800 awards per year. The single addition of FSCs 5961, 5998, or 5999 would more than double the current workload of CDAP, with minimal impact from the low volumes of 5963.

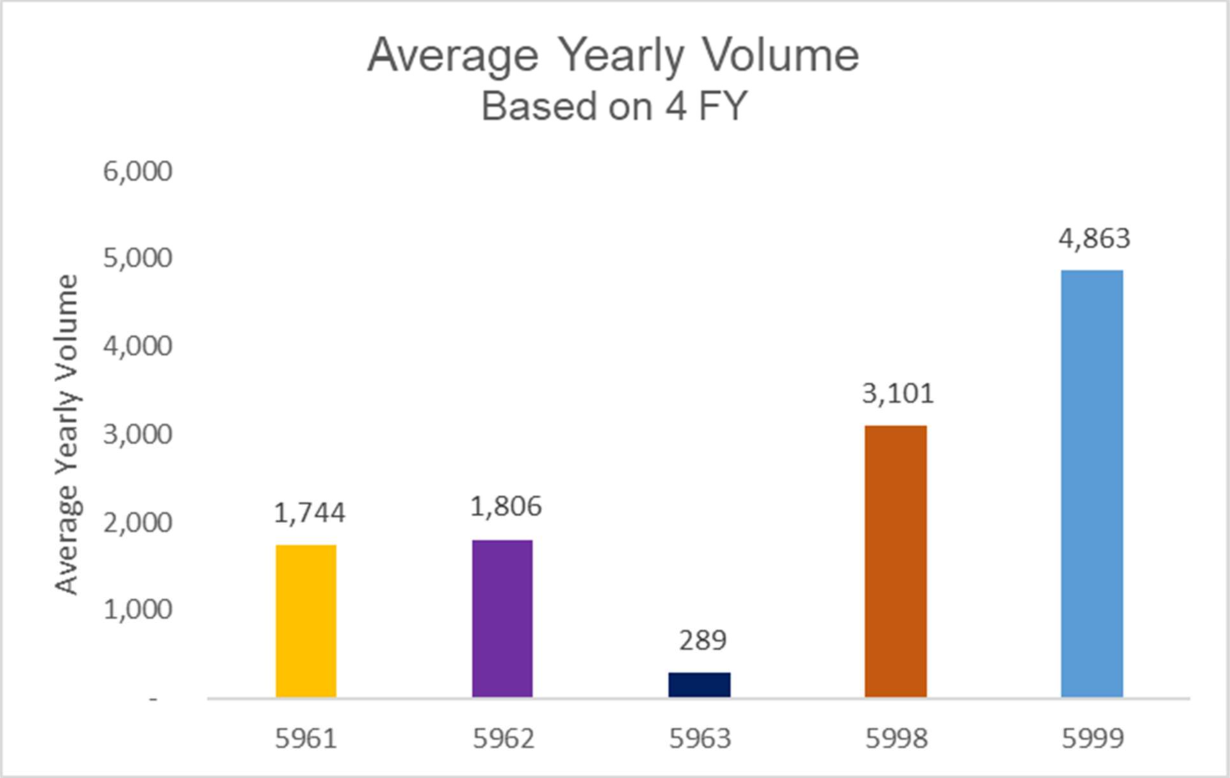


Figure 7. *Average Yearly Procurement Volume for Select FSC*

In addition, the cumulative increase in volume if all four proposed FSCs was also analyzed to understand the total impact to workload. Table 5 represents the cumulative volume of each identified FSC if they were added to CDAPs workload. Adding all four identified FSCs to the CDAP workload increases the total volume of awards needing review by approximately 553.5%, or approximately 5 times increase in volume.

Table 5. *Increase in Workload by FSC*

FSC	Volume of Awards per Year	Cumulative Total	% Change
5962	1,806	1,806	**-**
5961	1,744	3,550	**96.5%**
5963	289	3,839	**112.6%**
5998	3,101	6,940	**284.3%**
5999	4,863	11,803	**553.5%**

To ensure the integrity of the data, and representation of the types of awards entering the CDAP pipeline. The procurement data provided by J6 was scrubbed to only include appropriate document types. The 'Standard PO' document type is what is currently in the CDAP pipeline. These documents were kept in our data set, along with 'Auto-Award' document types. If the FSCs with 'Auto-Award' are added to CDAP, they would be moved to 'Standard PO' and enter the CDAP pipeline. The other documents shown in Figure 8 were removed from the data set, as they do not represent CDAPs current or future pipeline.

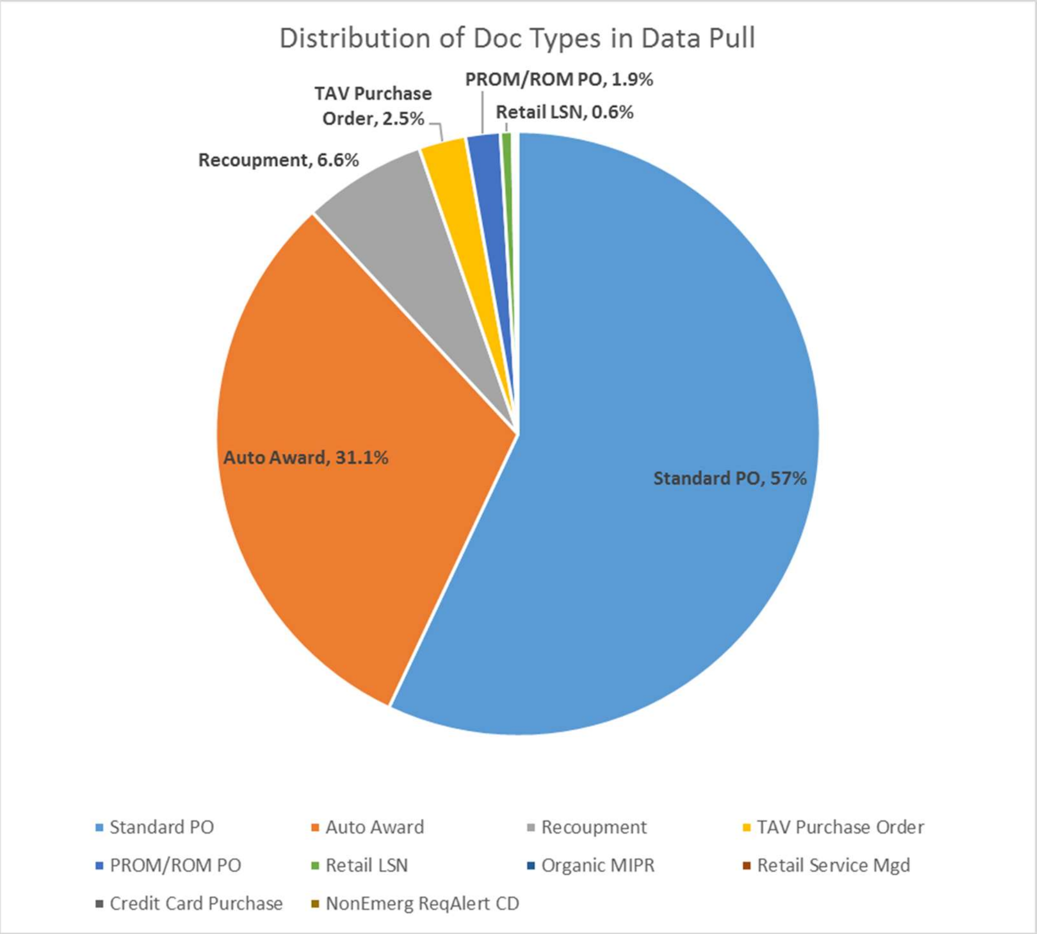


Figure 8. *Distribution of Document Types*

3.2.3.1 Benchmark Analysis

Once current state time estimates were confirmed, the model was designed with the intention of producing two outputs: the required work hours for completing a review and the required full-time equivalents (FTEs) necessary to handle reviews for each denoted FSC. Using the CDAP Catalog and J6 procurement data, the average amount of purchase orders for FSC 5962 were extrapolated and used as the yearly volume of reviews. The total time taken for a review was calculated through weighting time taken to review an error or error free traceability review; weights were obtained through information provided by stakeholders on how often errors are found. Ultimately, the volume of awards and the time taken were used as inputs to calculate total work hours needed per FSC in a year, and the FTE requirements.

The following formula was used to calculate the hours needed per review:

$$\frac{Chan\quad of\ No\ Error\ x\ Time\ for\ Clean\ Review + Chanc\quad of\ Error\ x\ N\ of\ Resubmission\ x\ Time\ for\ Error\ Reviews}{60\ mins}$$

In the above formula, the time taken for a completely clean review is calculated and is based off the assumption of an error occurring 50% of the time. The time for an erroneous review is also calculated with the number of resubmissions adding a weighted factor to reflect the true current state.

With real numbers substituted, the hours per review was calculated by:

$$\frac{(50\%\ x\ 30\ mins + 50\%\ x\ {\sim}2.5\ resubmissions\ x\ 60\ mins)}{60\ mins} = {\sim}1.5\ hours/review$$

Using procurement data for FSC 5962 (as well as others shown in appendix) and the sub-total of review hours per FTE, the yearly FTE requirement was calculated by:

$$\frac{Time\ per\ Review\ x\ N\ of\ Purchase\ Orders}{Subtotal\ FTE\ Capability}$$

Substituting data found throughout this study, the total FTE count for handling FSC 5962 is shown as follows:

$$\frac{1.5\ hour\ per\ review\ x\ 1{,}600\ Purchase\ Orders}{1{,}656\ FTE\ hours} = {\sim}1.5\ FTE$$

As shown in the findings section, CDAP is currently at capacity for handling FSC 5962 traceability reviews with a requirement of 1.5 FTEs.

3.3 CDAP Future State Capacity Analysis

The future state capacity analysis' objective is to assess the impact of (1) expanding the scope of CDAP to additional FSCs and (2) designing a future state model with enhanced processes and the impact of an expansion. The benchmark model was extrapolated to include the DLA identified FSCs and to analyze the impact if CDAP were to expand its scope under existing resources and processes. The process improvement opportunities identified during the current state analysis were quantified and incorporated into the model. This enhanced state was then expanded to the additional FSCs to analyze the workload impact.

3.3.1 Future State Capacity Assumptions

Assumptions for efficiency gains were created based on expected benefits of the implementation of a digital Form-918 as detailed earlier in this paper. The assumptions were analyzed, and efficiency factors were assigned based on DLA stakeholder feedback and research of industry standards. The major areas where assumptions were made for efficiency gains fall into the categories of data validation, automation, and business intelligence. Found in sections below, the assumptions, methodology for quantifying the assumptions, and application to the capacity model are explained. Figure 9 details the enhanced CDAP processes and is used to guide the following section.

1. Digital Web-form: The online web form includes data validation & built in controls to reduce vendor error during submission.
2. The CDAP Dashboard tracks upcoming PAR requests, allowing CDAP to manage their workload and assign tasks more easily
3. Analytic tools aid the CDAP resource in reviewing the traceability documentation by cross-checking the fields against DLA data such as the qualified vendor lists.
4. Automated notifications and messaging help CDAP resources communicate with external vendors when issues arise with their submissions
5. The digital form allows for easy digital signatures, and automatically will generate a notice to the Vendor instantly.

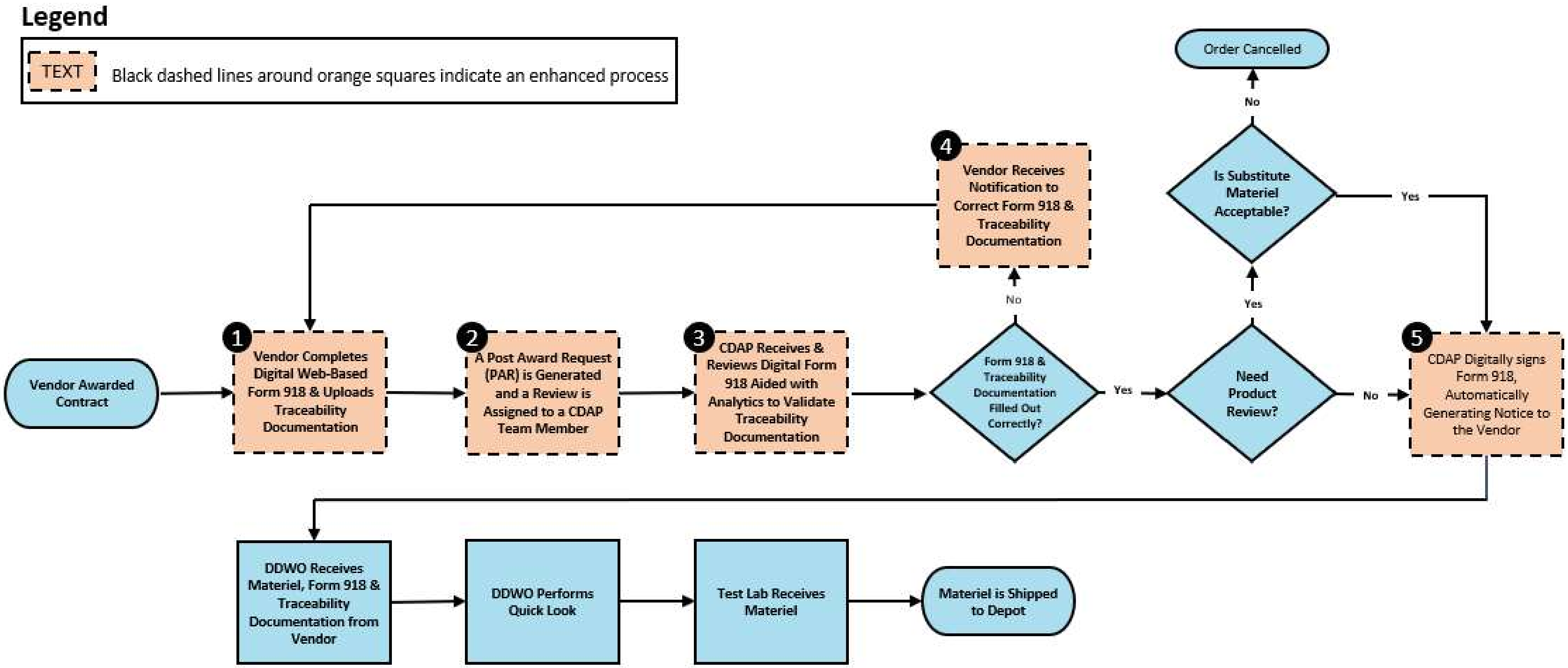

Legend
TEXT
Black dashed lines around orange squares indicate an enhanced process
Vendor Awarded Contract
1
Vendor Completes Digital Web-Based Form 918 & Uploads Traceability Documentation
2
A Post Award Request (PAR) is Generated and a Review is Assigned to a CDAP Team Member
3
CDAP Receives & Reviews Digital Form 918 Aided with Analytics to Validate Traceability Documentation
Form 918 & Traceability Documentation Filled Out Correctly?
No
4
Vendor Receives Notification to Correct Form 918 & Traceability Documentation
Yes
Need Product Review?
Yes
Is Substitute Materiel Acceptable?
No
Order Cancelled
Yes
No
5
CDAP Digitally signs Form 918, Automatically Generating Notice to the Vendor
DDWO Receives Materiel, Form 918 & Traceability Documentation from Vendor
DDWO Performs Quick Look
Test Lab Receives Materiel
Materiel is Shipped to Depot

Figure 9. *CDAP Future State Process Map*

3.3.1.1 Data Validation & Built in Controls

The existing state of CDAP's traceability review process, has an approximately 50% error rate of Form-918 submissions which significantly increases process times. The Digital Traceability effort has recommended the adoption of a digital web form with data validation and built in controls. The recommendation aims to minimize the opportunity for vendors to make mistakes when submitting Form-918 is essential to reducing the error rate of submissions.

A 90% reduction in the error rate is assumed in the future state model. The reduction in error rate results in less resubmissions, less communication, and faster traceability review times. The digitization of Form-918 will significantly free capacity and reduce inefficiencies of the CDAP process. This enhancement is estimated to reduce the time to review traceability documentation by 50% from 60 minutes when errors are approximately 50% to 30 minutes with an error rate of 10%. Errors cannot be 100% eliminated because it is extremely difficult to account for all types of extraneous circumstances. The types of mistakes that may be submitted with digital Form-918 are assumed to be circumstances such as when a substitute product is proposed and requires the review and acceptance of a product specialist.

3.3.1.2 Automation

The digitization of Form-918 to an online web-form enables the automated collection of data provided by vendors to CDAP. The automation of data entry increases data integrity, eliminating human error. In addition, with an automated data collection process in place, CDAP resources do not have to spend time performing manual data entry. The tables outlining the CDAP processes show that CDAP resources spend on average approximately 12 minutes performing data entry tasks for each award. Automating data entry provides a significant increase in FTEs available productivity time, due to the sheer volume of awards being completed each year. The elimination of manual tasks allows CDAP resources to focus their productivity on critical tasks such as reviewing the chain of custody of documentation, rather than spending time manually entering and reconciling databases.

3.3.1.3 Business Intelligence

The CDAP Dashboard is expected to provide workload management benefits to the CDAP stakeholders. In the existing state, data is manually shared, reconciled, and not in real time. The automation of data collection allows for CDAP to benefit from real time analysis and tracking of awards entering the CDAP pipeline. By tracking the lifecycle of an award, each stakeholder has visibility into each step of the process, and when an award may enter their respective pipeline. This transparency allows for managers to allocate resources more efficiently, ultimately increasing productivity of resources.

3.3.2.1 CDAP

The CDAP traceability review team realizes the largest impact from the process improvement opportunities. In the existing state, the approximately 50% error rate and resulting inefficiencies can increase the time to review a single award to approximately 90 minutes. In the future state, this error rate is nearly eliminated, and efficiencies gains from the various process enhancements result in an average 37 minutes to review traceability.

Table 6. *CDAP Future State Process Times*

CDAP - Future State	Time (min)
Review Digital Traceability	**30**
Form-918 (Required Fields)	15
Traceability Documentation	15
Sign & Send Shipment Notification	**7**
Signatures of Approval	2
Mail Documentation	5
Total Time	**37**

The future state assumptions and enhanced process times are incorporated into the model to reflect a future CDAP with digitized and enhanced processes. Determining the FTE requirement in the future state was like the current state calculations, with adjustments for the error rate, resubmission rate, and process times. The volume of awards did not change, the calculations are described below.

$$\frac{Time\ per\ Review\ x\ N\ of\ Purchase\ Orders}{Subtotal\ FTE\ Capability}$$

$$\frac{37\ minutes\ x\ N\ of\ Purchase\ Orders}{1{,}656\ hours}$$

The future state CDAP realizes a nearly 50% reduction in FTE requirements for each FSC, reducing the investment required in FTEs to expand CDAP to other high-risk FSCs. The results and comparison between the current state and future state FTE requirements are shown in Table 7. *CDAP FTE Requirements*

Table 7. *CDAP FTE Requirements*

FSC	Yearly Awards	Total Yearly Hours	Future FTE	Current FTE
5961	1,744	1,076	0.6	2.0
5962	1,806	1,114	0.7	2.1
5963	289	178	0.1	0.3
5998	3,101	1,912	1.2	3.6
5999	4,863	2,999	1.8	5.6

3.3.2.2 DDWO

The DDWO realizes the smallest impact from the process enhancements relative to the Traceability Review Team and the Test Lab. This is in part due to the DDWO's respective tasks that include a manual 'quick look' of the shipment and entering information into the QUID database. If an error is found, the DDWO generates a Supply Discrepancy Report (SDR), the process of which remains unchanged. The realized impact the DDWO experiences is mainly indirect. As such, reducing the CDAP Traceability Review Teams error rate and ensuring accurate data will result in less errors experienced by the DDWO. Therefore, the DDWO has a ‘clean future state’ and an ‘error future state’, both of which are shown in Table 8.

Table 8. *DDWO Future State Process Times*

DDWO - Future State Tasks	**Clean State**	**Error State**
Quick Look	10	15
Generate SDR Notification	0	10
Enter Information into QUID	5	5
Send Materiel to Test Lab	5	5
Total Time (minutes)	**20**	**35**

Table 9. *DDWO FTE Requirements*

FSC	**Yearly Awards**	**Total Yearly Hours**	**Future FTE**	**Current FTE**
5961	1,744	436	0.3	0.6
5962	1,806	452	0.3	0.6
5963	289	72	0.0	0.1
5998	3,101	775	0.5	1.0
5999	4,863	1,216	0.7	1.6

The following formula was used to calculate the DDWO FTE requirement:

The average time to complete an award is calculated by taking the weighted clean state time added to the weighted error state time, which is approximately 27.5 minutes for DDWO tasks.

$$(Percent\ chance\ of\ clean\ state\ x\ clean\ average\ process\ time) + (Percent\ chance\ of\ error\ state\ x\ error\ state\ average\ process\ time)$$

$$\big((75\%\ x\ 20\ minutes) + (25\%\ x\ 35\ minutes)\big) = {\sim}27.5\ minutes$$

The total workload hours in a given year is calculated by taking the average time to complete an award multiplied by the volume of the given FSC. This output is divided by 60 minutes to derive the total time in hours.

$$\frac{Average\ time\ to\ complete\ an\ award\ x\ volume\ of\ awards}{60\ minutes}$$

Determining the required FTE for each FSC requires the previous calculation of total yearly workload in hours divided by the yearly availability of an FTE, estimated at 1656 hours.

$$\frac{Total\ hours\ requried\ in\ a\ year}{1{,}656\ hours} = requried\ FTE\ estimate$$

The estimated FTE requirement for each FSC in the future state is below.

Table 9. *DDWO Future State FTE Requirement*

FSC	Yearly Awards	Total Hours (yr)	FTE's Req.	Cumulative FTE Req.
5961	1,744	436.1	0.3	0.3
5962	1,806	451.6	0.3	0.5
5963	289	72.4	0.0	0.6
5998	3,101	775.4	0.5	1.0
5999	4,863	1,215.9	0.7	1.8

3.3.2.3 Test Lab

The Test Lab experiences significant gains in efficiency due to the bottlenecks associated with the lack of data integration and inefficient communication with internal and external stakeholders. The largest impact is realized within the Test Lab's traceability review process. The future state data integration and increased communication efficiency decrease the time to review substantially. Indirectly, the Test Lab will experience less documentation with errors due to the digitized web-based Form-918's built in controls and data validation when collecting data. The weights used in the calculations are 90 percent error free and 10 percent chance of errors present. Table 10 reflects the improved process times for Test Lab tasks.

Table 10. *Test Lab Future State Process Times*

Test Lab - Future State Tasks	Clean State	Error State
Unpackage Materiel	10	20
Review Traceability Documentation	5	30
Enter Data into QUID	5	10
X-Ray	10	10
DNA Marking	20	25
Baking Components	5	5
Repackage Materiel	10	20
Send Materiel to Depot	5	10
Total Time (minutes)	**70**	**130**

The following calculations were used to determine the FTE requirements for the Test Lab.

The average time to complete an award at the Test Lab is calculated by taking the weight of the clean state multiplied by the clean state average time and adding it to the weight of the error state multiplied by the error state average time.

$$(\%\ Weight\ of\ Clean\ State\ x\ Clean\ State\ Average\ Time) \\ + (\%\ Weight\ of\ Error\ State\ x\ Error\ state\ Average\ Time)$$

$$(90\%\ x\ 70\ minutes) + (10\%\ x\ 130\ minutes) = {\sim}76\ minutes$$

The total workload hours for a given year is calculated by taking the weighted average time to complete Test Lab tasks multiplied by the total volume of each FSC.

$$Weighted\ Average\ of\ Test\ Lab\ Process\ Times\ x\ Volume\ of\ Awards$$

The required FTE estimate is calculated by taking the total workload hours and dividing it by the FTE availability hours, estimated to 1,656 hours per year.

$$\frac{Weighted\ Average\ of\ Test\ Lab\ Process\ Times}{1{,}656\ Hours}$$

The estimated FTE requirement for the future state Test Lab is shown in the table below.

Table 11. *Test Lab future State FTE Requirement*

FSC	Awards per Year	Total Hours (yr)	FTE's Req.	Cumulative FTE Req.
5961	1,744	2,209.1	1.3	1.3
5962	1,806	2,287.6	1.4	2.7
5963	289	366.1	0.2	2.9
5998	3,101	3,927.9	2.4	5.3
5999	4,863	6,159.8	3.7	9.0

3.4 Conclusion

The Counterfeit Detection & Avoidance Program (CDAP) is working at capacity to review traceability for high-risk electronic microcircuits in FSC 5962. DLA leadership seeks to expand the scope of CDAP beyond FSC 5962 and has identified four additional FSC's to potentially add to the program. However, CDAP stakeholders cannot meet the demand of additional high-volume FSCs without increasing capacity through process improvements or additional resources. The lack of capacity to expand to additional FSC's can be contributed to several factors:

- Manual paper-based processes
- Inefficient communication between internal and external stakeholders
- Lack of system integration and inefficient data sharing between internal and external parties
- High error-rate of vendor submissions resulting in cycles of resubmission

The result is an inability for CDAP to expand its program beyond FSC 5962, leaving other high-risk FSCs vulnerable.

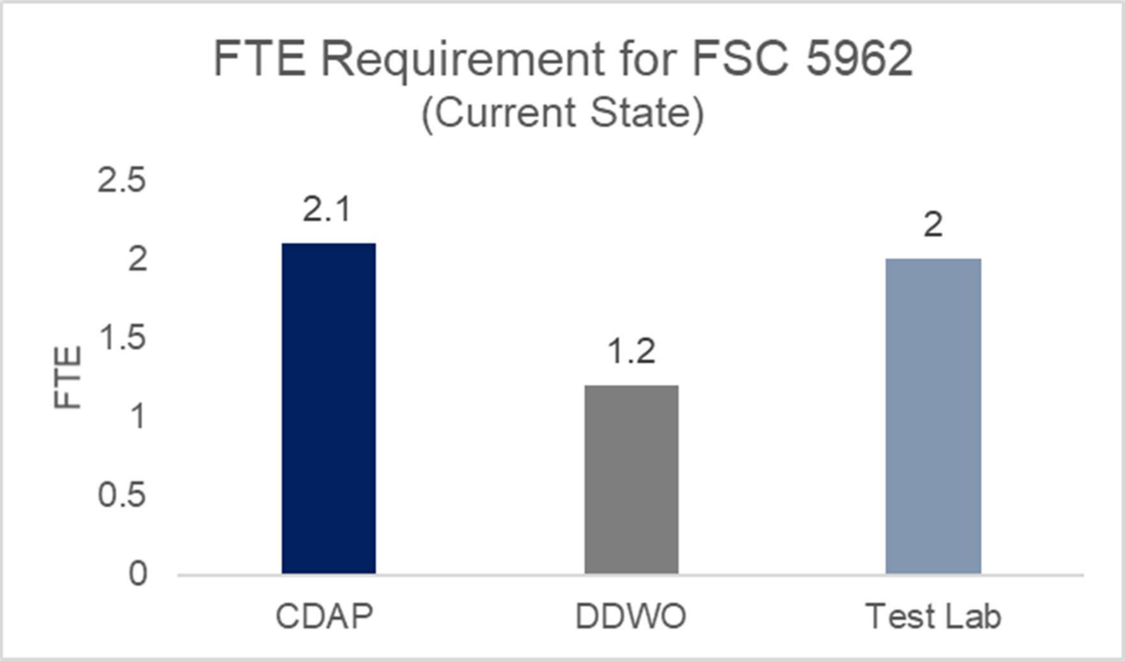


Figure 10. *Current State FTE Requirement*

Analysis of the workforce capacity model findings identified opportunities for CDAP to expand its scope by improving processes and adding additional FTEs to CDAP. The opportunities identified and incorporated into this analysis include:

- Reducing the error rate of vendor submissions by digitizing Form-918 with data validation and built-in controls
- Streamlining communication by reducing the dependency on e-mail communication and increasing transparency of CDAPs pipeline through workload management dashboards
- Automating data collection and storage to eliminate manual processes and integrating CDAP data internally and with DLA's Enterprise Data Warehouse (EDW) to streamline data sharing

Investing in improving CDAP's processes will increase resources efficiency and reduce the overall lifecycle of an award in CDAP's pipeline. Reduction in the lifecycle of an award, gives CDAP additional slack in its capacity with existing resources. Thus, CDAP could expand its scope to an additional FSC without adding additional resources.

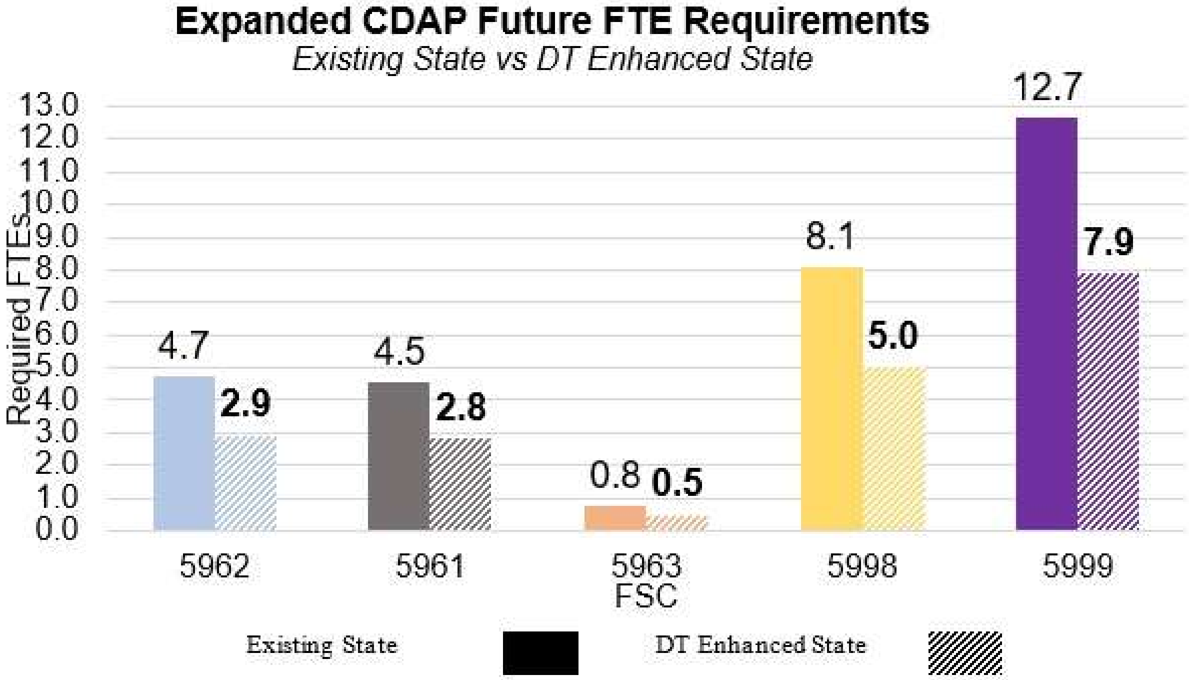


Figure 11. *Expanded CDAP Future State*

Expanding the scope of CDAP to FSC 5961 is possible without increasing FTEs. This expansion would not be possible without process improvements due to the constraints of the existing CDAP process. In addition, improving CDAP processes enables the expansion to other identified high-risk FSCs while reducing the overall FTEs required to handle larger award volumes. As shown in the graph below, an improved CDAP process reduces the overall investment compared to CDAP without any improvements.

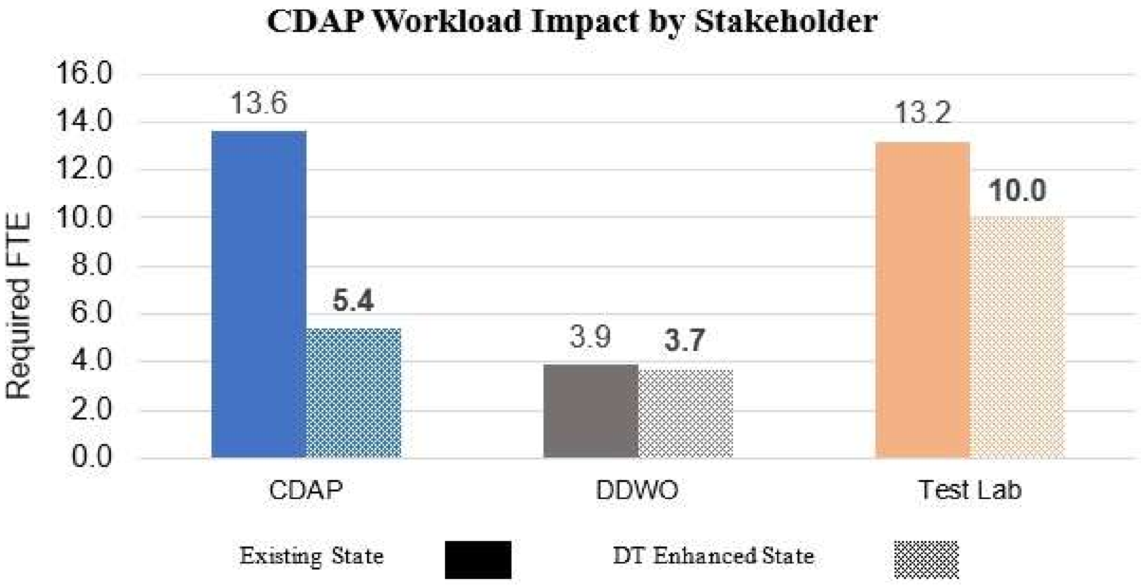


Figure 12. *CDAP Workload Impact by Stakeholder*

Until DLA invests in improving CDAP processes and increasing resource capacity, the scope of the program should not be expanded to additional FSCs without significant investment in additional resources to meet the demand of awards requiring traceability.

4.0 Enhanced CDAP Data Storage Plan

As the Counterfeit Detection and Avoidance Program continues to operate and expand, there is an increasing need for program data to be recorded and retained in an enterprise environment. Not only does enterprise storage allow the data to be accessed more easily by participating user groups, but this type of storage also provides disaster recovery support, real-time information, and data accessibility for use in a broad variety of business intelligence platforms. Additionally, and importantly, enterprise storage also provides an easily auditable method for reviewing past records as needed.

To help enable more efficient, accurate, and timely data sharing, it is recommended that the CDAP Catalog data (and any other relevant business information) be integrated with DLA's enterprise data systems, namely the Enterprise Data Warehouse (EDW). Integrating CDAP data into the EDW will allow access for all CDAP stakeholders in real time, and would enhance visibility across the enterprise, opening opportunities to improve CDAP and utilize business intelligence tools.

CDAP data is currently stored locally on a shared drive, which is susceptible to system failure and loss of data. Should the shared drive fail, or a catastrophic error occurs, it may be impossible to retrieve the data causing an unknown amount of work stoppage and delays. Additionally, locally stored files are also prone to user error and are rarely archived or backed up when compared to an external server or cloud database. Therefore, to ensure the integrity and security of data, it is recommended that the CDAP should move away from local storage of data to an enterprise wide data structure including storage within the Enterprise Data Warehouse.

4.1 Existing CDAP Databases

The CDAP process is highly collaborative and is supported by different internal stakeholder groups including the CDAP Management Team, the Test Laboratory, Warehousing, and Procurement. Each group is responsible for at least a portion of the CDAP process and these parties share information about the status of each procurement and review. Currently, the definitive record of each CDAP review is tracked in a database called the CDAP Catalog. However, there are other databases used by participating groups such as the Test lab, which also track important aspects of each review such as the inspection and testing results. These key databases are often siloed and keeping track of the most up-to-date information for each procurement record can be challenging. Some of the key CDAP databases and the user groups who rely on them are depicted in the figure on the next page.

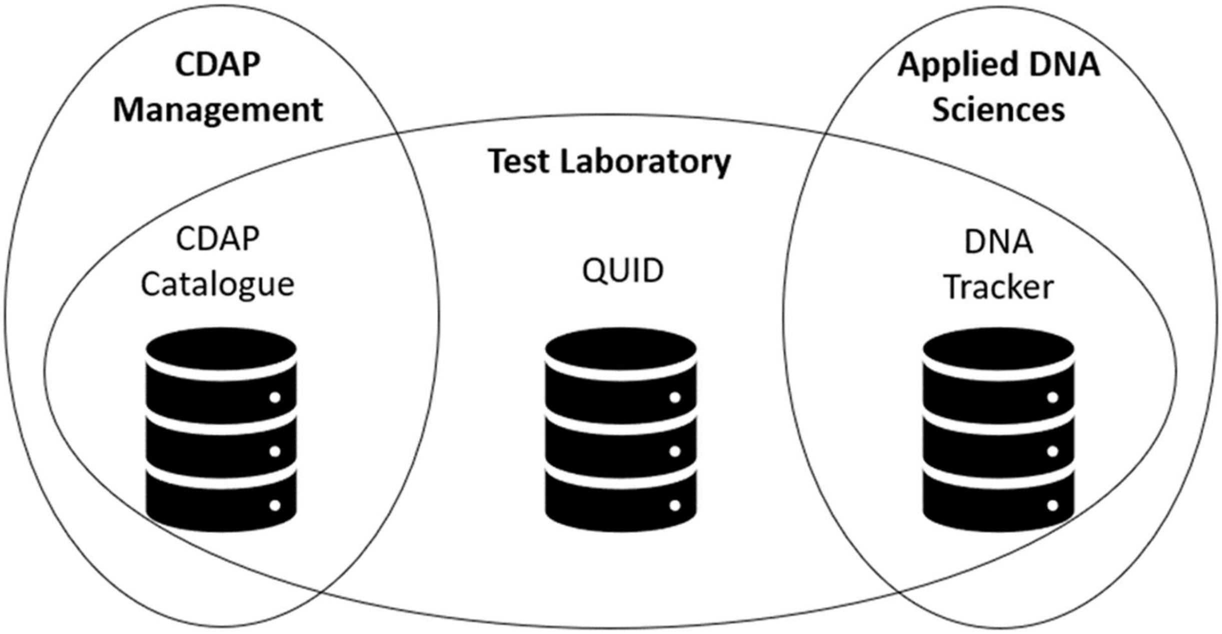


Figure 13. *CDAP Databases*

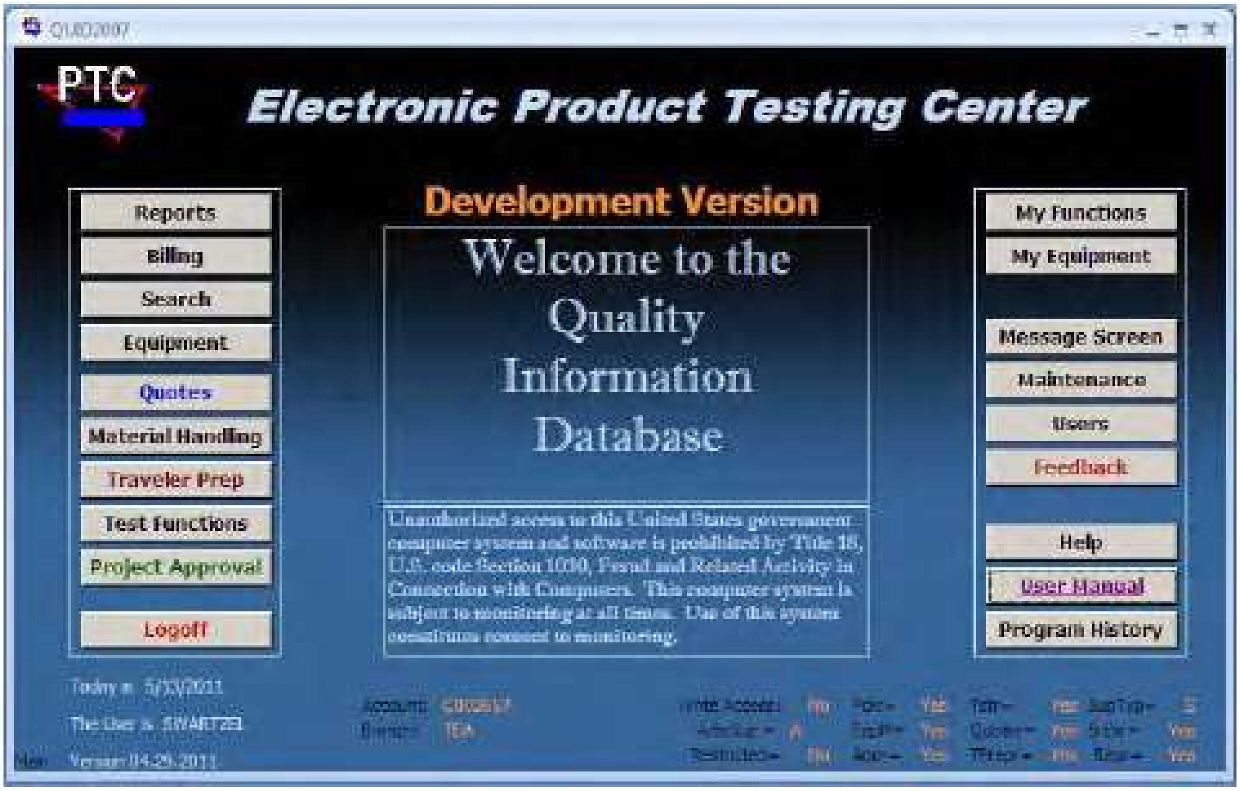
4.1.1 CDAP Catalog

Currently, the definitive record of each CDAP review is tracked in a database called the CDAP Catalog, which is updated often and shared via manual updates between user groups. However, there are other databases used by participating groups such as the Test Lab, which also track important aspects of each review such as the inspection and testing results. While relatively small manually updated databases may be effective at the current scale, the CDAP Catalog – which is built as a Microsoft Access database – does not connect to an enterprise database and is not ideal for potential future program expansion.

4.1.2 Quality Information Database (QUID)

The Test Lab at DLA L&M is tasked with performing inspections and DNA marking electronic microcircuits within the CDAP process shortly after they are received. Test Lab resources utilize multiple disparate databases to perform their respective duties and track results of their testing and marking activities. The Quality Information Database (QUID) is the main database used for most Test Lab tasks and was built using Microsoft Access.

QUID is used to track the lifecycle of projects within the Test Lab. This includes creating a unique project ID and subsequently tracking each step of the process creating a log of activities and information regarding the specific project. As the main Test Lab database, QUID helps perform and track a variety of information regarding the testing and marking of FSC 5962 components.



Unauthorized access to this United States government computer system and software is prohibited by Title 18, U.S. code Section 1030, Fraud and Related Activity in Connection with Computers. This computer system is subject to monitoring at all times. Use of this system constitutes consent to monitoring.

Today is 5/13/2011
The User is SWARTZEL
Version 04-29-2011

Figure 14. *Quality Information Database Main Screen*

The QUID front end application allows Test Lab users to easily access different modules to complete their daily tasks. An important function of QUID is the ability for users to query the database to generate custom reports and data for deeper analysis. The database also tracks a log of activities for each respective project, tracking the full life cycle of an award within the Test Lab. Users can share notes and information within QUID, including the ability to communicate with supervisors for approval prior to conducting operations. QUID acts as the central system for all Test Lab functions and is integral to their success.

As the central system for tracking Test Lab activities, the database has shortcomings in that it is not connected with DLA's Enterprise Data Warehouse (EDW). The information used by the QUID functions pulls data from a variety of tables housed in QUID called QUIDTables. Information that is not housed or collected by QUIDTables must be manually entered by users or uploaded from spreadsheets.

4.1.3 DNA Tracker

DNA Tracker is an access database that is used to track DNA information of projects, and is used as a communication medium between ADNAS and the Test Lab. This database is linked to QUID and tracks the actual marking sessions and DNA information exchanged between ADNAS and the Test Lab.

4.2 Future Consolidated CDAP Database

The existing Test Lab database solution lacks integration with other CDAP databases and DLA's Enterprise Data Warehouse (EDW). The lack of integration and offline nature of the database creates a bottleneck in certain test lab processes. The review of traceability documentation by the test lab requires resources to access their own data sources as well as the CDAP Catalog to verify the chain of custody of electronic components. Information that is not housed in the QUIDTables must be manually entered into the database causing increased time to complete tasks and hindering data integrity. The DNA Tracker is also not integrated with any systems and is used to share data with the external third party, ADNAS. This lack of integration with ADNAS makes data sharing difficult and time consuming. The Test Lab can become backlogged if ADNAS takes longer to share the necessary DNA marking information and can take several days to update the database.

Although the lack of integration causes several issues for the Test Lab, having an offline database has provided benefits as well. The tradeoffs described above are offset by allowing the test lab to have greater autonomy over its data. Test Lab resources can query and analyze data on an ad-hoc basis, rather than requesting a data pull from J6. Resources can also establish their own requirements and modify the fields and data being collected as needed. A future solution for the Test Labs database system should solve the issues described above, and still allow the Test Lab to perform its daily functions with accurate and accessible data.

The QUID and DNA Tracker Access Databases should be integrated into DLA's enterprise data warehouse (EDW) and the CDAP Catalog. Consolidating these databases provides a variety of benefits and future opportunities for the Test Lab and CDAP.

4.2.2 Future CDAP Database Benefits

4.2.2.1 Data Integrity

Bringing the Test Lab's databases online and connected to DLA's EDW and CDAP's CDAP Catalog can automate the collection of data and increase the scope of the data collected due to its integration with enterprise systems. Test Lab resources are guaranteed that the data collected is as accurate as possible and eliminates the need to reconcile data.

4.2.2.2 Workload Management

Integrating the Test Lab's data with the CDAP Catalog can provide greater visibility into the lifecycle of an award. Awards can be tracked from the initial traceability review conducted by CDAP to the end process of testing and DNA marking components. Business Intelligence dashboards can be utilized to gather deeper insights into this larger set of data. Integration into DLA's EDW stores CDAP and Test Lab data into its powerful systems, allowing for real time updates, data pulls, and reporting. Greater visibility into the lifecycle of an award allows CDAP to better understand its existing and upcoming pipeline to better manage workload.

4.2.2.3 Reduced Manual Actions

A key function of the Test Lab is to conduct a secondary traceability review of FSC 5962 awards. Integrating its database with CDAP and EDW allows the reviewer to access all the necessary data in a central location rather than accessing multiple, separate databases. Centrally accessing procurement data, CDAP data, and general supplier information that may be housed outside of the Test Lab or CDAP can impact the time it takes to review traceability documentation and allow the Test Lab to focus on core functions such as testing and DNA marking. In addition to accessing data, the automatic collecting of data eliminates the need to manually enter information. Manual data entry is a time consuming and removes resources from performing core functions. Overall, the integration of systems and automatic data collection will reduce the time to review traceability and allow resources to focus on core functions.

4.2.2.4 Streamlined Communication

The Test Lab communicates with two parties to perform its core functions, ADNAS and CDAP. Communicating with ADNAS involves sharing an offline spreadsheet with DNA Marking data. The Test Lab must wait for ADNAS to update the spreadsheet with the necessary DNA Marking information, which the Test Lab cannot mark parts without. The sharing of data between these two parties can cause a backlog in the Test Lab. ADNAS can take several days to provide the Test Lab with the necessary information, often resources are left in the dark and are unsure when they will receive the update from ADNAS.

Communications with CDAP are primarily for the second traceability review. If issues arise during the review, Test Lab resources will access the CDAP Catalog or reach out to a CDAP resource to confirm discrepancies or information. An integrated Test Lab database would allow for Test Lab reviewers to access CDAP data in a central location that is up to date and does not require data reconciliation.

4.3 CDAP Database Requirements

It is recommended that DLA integrate the Test Lab’s QUID and DNA Tracker databases with DLA’s Enterprise Data Warehouse and CDAP Catalog. This integration will modernize the IT infrastructure of the Counterfeit Detection & Avoidance Program (CDAP).

The Test Lab Databases should be integrated with the CDAP Catalog, adding the unique data fields used by the Test Lab to the CDAP Catalog. Integrating the Test Labs databases with the CDAP Catalog provides a starting point for creating a central CDAP repository that has visibility into the full lifecycle of an award. This centralized database should be integrated with DLA’s EDW to reduce the strain of database maintenance on CDAP resources. In addition, integration with EDW allows for real time updates, and access to CDAP data to other DLA departments. As departmental processes, data elements, and procedures may change over time, it is recommended that all three database elements be preserved in a future state database, as determined by process area leads. These recommendations are in line with the recommended requirements laid out within this document.

5.0 Contingency Planning

Contingency planning is essential to the maintenance and operation of any critical business function relying on technological processes and/or systems. Contingency plans are prepared documentation describing how potential interruptions or outages may be mitigated by means of alternate processes, systems, or issue resolutions. Within the scope of proposed Digital Traceability enhancements, it is necessary to have both enterprise and CDAP-level contingency plans. Enterprise plans will address any high-level system outages which may impact end user internet and/or data access, while CDAP-specific plans may address more discrete scenarios specific to the program's process steps.

5.1. Enterprise Continuity of Operations Plan (COOP) / Disaster Recovery (DR)

One major benefit of bringing the Counterfeit Detection and Avoidance Program data into an enterprise environment is the overarching Continuity of Operations Plan (COOP) and Disaster Recovery (DR) protection provided to DLA enterprise environments. These enterprise contingency plans are part of the wider Concept of Operations (CONOPS) and Production Support provided to DLA's Enterprise Business Systems (EBS) by the Defense Information Systems Agency (DISA). All COOP/DR plans detailed in this section for EBS are current as of DISA's CONOPS V.0.93 document dated November 22, 2017. Details of DISA's support to DLA, as described in this document are described as follows:

"DISA provides full range Premium Support services to mission partner Defense Logistics Agency for the EBS Production and EBS COOP environments. DISA's Premium Service goes beyond supporting just SAP applications, it provides end-to-end support of DLA's entire platform, including mission-critical customer and partner applications. Through partnered liaison, the service is designated to accommodate scheduled maintenance, change management, and issue resolution for infrastructure, server/system administrator, database administration, batch job scheduling, application support, and system monitoring."

Complete documentation of DISA's EBS CONOPS for DLA's Production environments is available upon request. For convenience, relevant information from this documentation is provided in sections below. Information in these sections copied exactly as it appears in the original documentation (section numbering excepted).

5.1.1 EBS Concept of Operations (CONOPS)

Maintenance of the EBS Production environment includes the business application components, and infrastructure/applications performing data synchronization between the EBS Primary sites at DECC Primary and the EBS alternate site (or "COOP site") for disaster recovery.

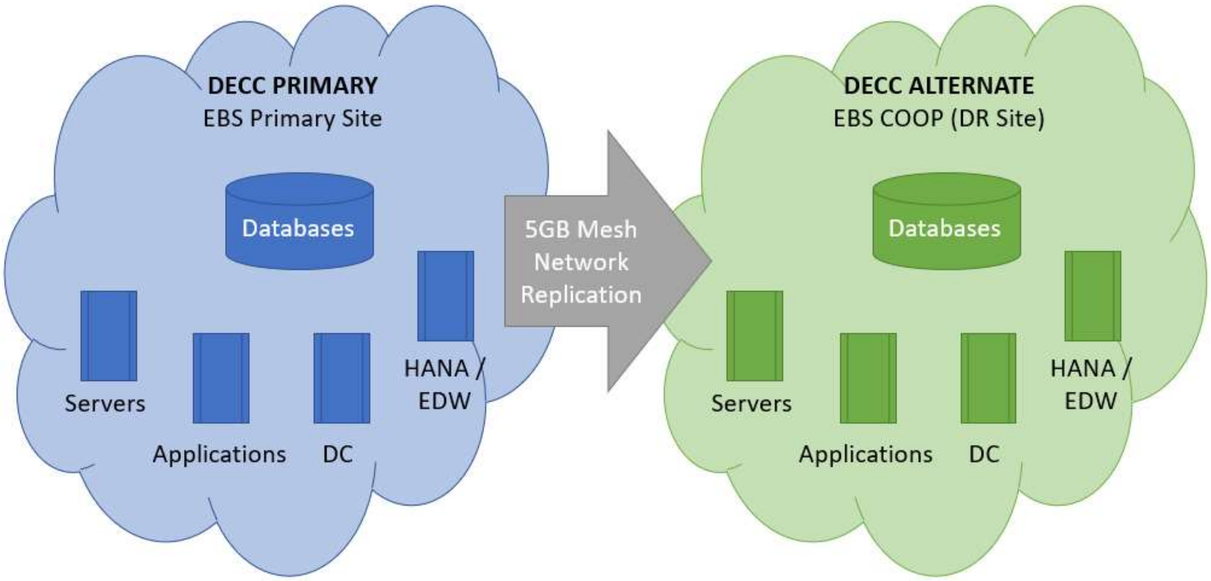


Figure 15. *EBS Primary and COOP Sites*

The EBS environment at the COOP site is designed to function as a "Mirrored Site" for Primary EBS Production Site, per the definitions of alternate sites. (NIST Special Publication 800-34 Contingency Planning Guide for Information Technology Systems).

5.1.2 COOP CONOPS

The COOP site remains in "standby mode", (where databases are read-only, and applications are not accessible by users during normal conditions) and is kept in sync with the primary site by automated data replication as well as manual change management operations.

In the event of a major service interruption (either planned or unplanned) in the EBS primary production datacenter, failover procedures will bring the alternate COOP site into "production mode", ready to take the place of, and fully support the workload of the primary site with minimal time/effort from DISA and DLA Operational support staff. The Ogden Disaster Recovery team provides this guidance for a Failover Procedure, with the order of operations as follows:

1. Notification of Problem (either mission partner to service desk, or vice versa (depending on who notices the issue first)).
2. A trouble ticket is created
3. Local restoration efforts take place (depending on the scale of the event).
4. Go/no-go decision to start COOP operations – generally 25% of the RTO for the application (i.e. 6 hours for an application with a 24 hour RTO).
5. Decision rests with Ecosystem Chief (since it requires resources from multiple LOBs) – would generally be done in consultation with the mission partner and the LOBs involved.
6. For large scale disasters, recovery is prioritized by RTO associated with the COOP solution purchased.
7. Return to original production site is handled as a planned migration with ASI notifications and generally on the weekend or during the application's maintenance window.

A note on what constitutes a COOP level event – it used to be only a loss of access to the servers (for whatever reason – loss of power, hardware, network, etc.), but it has been expanded to include cyber considerations (for example if the mission partner has reason to believe that their production environment has been hacked).

Authority to order a Failover (to switch EBS Production workload from a Primary site to an Alternate/COOP site) requires consensus by DISA and DLA executive management. A valid Failover "Go-No-go" decision must be obtained in writing from the DISA Special Services Lead and DLA J62EA (Information System Contingency Plan (ISCP) Enterprise Business System (EBS) DISA Hosted COOP V.1.6 April 25, 2017 Section 3, page 24 and Appendix B.1 Leadership and Supervisors, P 41).

Once a decision has been made to execute a failover, designated DISA and DLA teams complete a failover checklist (EBS STL-to-OGD Live Failback Schedule_MASTER_20170825_1445). The Service Integration and Delivery (SID), team will track the completed tasks for the failover and report status to all stakeholders accordingly, to ensure seamless awareness.

Periodic COOP exercises, (tabletop and/or live simulations) will be performed in coordination with the DISA Disaster Recovery Team per the terms of the 2017 EBS DISA Hosted COOP April 2017 V.1.6 (See ISCP APPENDIX L: TEST AND MAINTENANCE SCHEDULE page 67).

5.1.3 Enterprise Service Operations

Enterprise Service Operations and Incident/Event Management are important aspects of how disruptions in service or operation are handled. The following information within this section (5.1.3) are copied exactly as they appear in DLA/DISA CONOPS documentation. Full text and additional service outage scenarios (outside of scope of CDAP teams) are available by request.

5.1.3.1 Service Desk

The PRC Service Desk is a Level 1.5 single point of contact function, hosted out of the primary production site, with 24/7 support. It is a functional unit with staff trained and capable of resolving routine support requests, receiving and cataloging incident reports, and properly escalating issues to the appropriate Level 2 group if an incident is not resolvable. End-users of mission partner applications will need to contact their designated Mission Partner Service Desk for incidents regarding the application. If it is determined that there is an issue with the EPC Service, then the Mission Partner's Service Desk will create an ITSM ticket and route it to the EPC Service Desk. The EPC Service Desk is required to escalate incident tickets to Level 2 support groups. COOP escalation of incident priority is also required to ensure service levels can be met in the event of a COOP scenario.

5.1.3.2 Service Levels

The EBS Primary (Production) environment operates as production at a Mission Assurance Category (MAC) III level. This includes data recovery and COOP capabilities set with both Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) at 24 hours.

- **Recovery Time Objective (RTO)** – is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
- **Recovery Point Objective (RPO)** – describes the acceptable amount of data loss measured in time.

The following service level targets apply to the COOP service in order to support the RTO/RPO:

- **EPC Service Desk operations:** 24 hours, 7 days per week.
- **Incident Response time:** The amount of time elapsed after an incident is assigned to a technician.
    - Critical impacting incident: 4 hours
    - High impacting incident: 24 hours (Federal workdays, 0800-1800 ET)

5.1.3.3 Incident Management

Incident Management is responsible for managing the lifecycle of all incidents. An incident is defined as an actual or perceived interruption or reduction in quality of an IT service. In incident management, the goal is to restore normal service operation quickly while minimizing adverse impact to business operations. Furthermore, it ensures the best possible level of service quality and availability are maintained within SLA limits.

EBS Incidents are initiated and tracked in the EPC ITSM ticketing system. Incidents occurring in the EBS COOP environment are managed at a lower priority level than incidents occurring in the production environment due to the minimal impact to end users in COOP. Within the production environment, potential business functional impact may occur after 24 hours of unavailability of a service. The primary impact to COOP is to the data replication caused by communication loss. This may be caused by network, server, database, or application incidents. Collaboration calls are not initiated due to a lack of user impact. Broadcast messages and InfoSpots are not created due to a lack of user impact. Technical calls can be initiated for high tickets. A daily ITSM ticket report should be established to report tickets in breach of service levels. Reference document DISA Terms and Conditions v 6.3.1 June 2017 for more information.

5.1.3.4 Problem Management

Problem Management is concerned with managing the lifecycle of all problems. A problem is defined as the unknown cause of one or more incidents. The goal of problem management is to prevent problems and resulting incidents from happening again, eliminate recurring incidents, and minimizing the impact of incidents that cannot be prevented. Problem Management operates at the same service level in COOP as in production.

InfoSpots will not be created for the COOP environment except in cases of critical incidents which would impact all of COOP at a complete loss to the environment. The mission partner requirement of InfoSpots requires a root cause analysis for user impacting incidents which is a function of problem management. InfoSpot deployment is not delayed if the root cause has not been determined. It can be included on the InfoSpot after the event, and the DISA RCA INFOSPOT Chart report is emailed every morning listing InfoSpots that do not contain a root cause and the owner (submitter) of it. This is done to track and remind people to get an update the root cause as quickly as is reasonably possible.

5.1.3.5 Event Management

Event Management is a function that covers the tracking events throughout their lifecycle. Event notifications can be created by automated monitoring tools, or system administrators. Monitoring tools may generate events for a variety of reasons including faults, thresholds, configuration changes and informational. Events are reviewed by the appropriate supporting operations team, often the Service Desk, to determine their impact severity. Service impacting events become incidents for tracking purposes, even if they are cleared immediately following notification.

5.1.3.6 Network Monitoring

Successful continuous replication is critical to fulfilling the SLA. Reliable network operations are critical to successful replication. Network issues between Ogden and the COOP site should be assigned highest priority status and addressed immediately.

Domain and network issues are critical components to the normal business operations of DLA and DISA. These issues also impact the replication processes. Domains are susceptible to Distributed-Denial-of-Service (DDoS) attacks. A DDoS attack is defined in the "PM Memo COMM LOB DDOS Measures" draft document as:

Definition of a DDOS Attack: *"In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting a particular computer and its network connection, or the computers and network of the sites mission partners are trying to use, an attacker may be able to prevent access to email, websites, applications or other services that rely on the affected computer or network."*

Network performance should be monitored in real-time and reported to DISA and DLA teams on a daily basis. Regarding WAN connections between COOP and PROD, DISA monitors all of their links with Spectrum. This does not perform active performance monitoring, just the state of the link (up or down). DISA said that they can pull performance reports if needed, however, any monitoring of the internal DLA network would be a paid service.

5.2 CDAP Contingency Planning

The Counterfeit Detection and Avoidance Program facilitates an important anti-fraud role in the procurement process for DLA's most at-risk components. As such, it is of paramount importance that the program remains operational in circumstances where technical difficulties may arise. Furthermore, an enhanced technical footprint (i.e. reliance on a new or increased amount of technology) may expose the program to additional potential outages should new systems and/or integrations be implemented. For these reasons, the CDAP team requires a contingency plan which describes methods for CDAP to remain operational during various potential technical outages.

In the event of an outage, having a contingency plan in place will help minimize delays, potential backorders, and work-stoppages. If any system becomes inaccessible to either external or internal users, or both, a contingency plan will provide instructions to ensure that there are alternative options for continuing operations.

5.2.1 Planning for Future Platform

While no specific platform is being recommended, it is a finding of the Digital Traceability project that future CDAP data collection should be performed with a digital platform. Many such platforms are available which can serve the needs of the CDAP team, and platform-specific contingency planning will be required once a production platform is chosen and deployed.

In selecting a platform, DLA J6 will likely assess aspects of security, functionality, and resiliency. The chosen platform will also very likely be required to be FedRAMP (Federal Risk and Authorization Management Program) certified to collect and process sensitive data on a secure cloud environment. Once a platform is chosen, separate contingency planning activities should occur to prepare for potential outages and/or unexpected errors within the system. Where possible, it is recommended that manual backup processes be documented.

5.2.2 Contingencies for Core CDAP Processes

The contingency plan for CDAP aims to account for downtime on any current systems (i.e. DLA Email and eProcurement) as well as recommended future state systems (i.e. Vendor-facing portal and Workload Management). Overall, seven potential failure modes were identified which require contingency planning. The seven identified points of failure (susceptible to breaking or being offline) for a future Digital Traceability capability are:

1. Vendor-facing portal (***Future State***)
2. DLA Email systems (***Current and Future States***)
3. Automated Communication System (***Current and Future States***)
4. Workload Management System (***Future State***)
5. Data Storage (***Current and Future States***)
6. eProcurement (Contracting) System (***Current and Future State***)
7. Individual CDAP User Computer/Email (***Current and Future State***)

These potential points of failure are discussed in order of potential impact to CDAP operations and external communication from most important to least important to address. It is important, for example, for vendors to have access to the future state portal for timely updates on approvals and authorization to ship goods. It is less impactful to CDAP, but still important, for the contracting system of record to be operational.

5.2.2.1 Vendor-Facing Portal

The highest priority potential outage is that of the future state vendor-facing portal. As recommended, such as portal would help facilitate the collection of data from vendors, as well as provide them with a means for tracking the status of their purchase orders. In the event that this portal is inaccessible or down, vendors will have to communicate with CDAP Management directly via email, the US Postal Service, or telephone. In preparation for such a contingency, contact information for CDAP representatives should be provided within the portal during normal operation, and included with any official correspondence via email, USPS, etc. Additionally, if possible, appropriate contact information should be provided on ‘system outage’ screens prepared for such occurrences. In the case where the portal is down, a vendor would be able to see confirmation of a system error and appropriate contact information for moving forward with the

CDAP process. In this scenario, the backup for the vendor portal being down will ultimately be a reversion to email, telephone, and USPS for communication with vendors.

Initial Resolution Step(s): When any CDAP team member is informed that the vendor-facing portal is inaccessible, they should verify the outage by attempting to access the system. If the vendor-facing portal is down, contact a J6 Information Operations representative or call the Enterprise Help Desk to report the outage.

5.2.2.2 DLA Email systems

It is possible that DLA Email systems will fail on an enterprise or site-level, leaving the entire CDAP team without access to electronic communications. Although this scenario is already covered under enterprise contingency backups, this only ensures the resolution will be worked immediately, but downtime may still occur. Therefore, the CDAP response to this type of outage should focus on continuity of operations as opposed to confirmation and reporting of the outage. In a situation where email systems are down, CDAP team members will still have access to data records and should continue to operate as expected. In this scenario, CDAP Management resources should review 'active' records to determine whether any vendors are expected to be submitting traceability and/or Form 918 documentation. In the case where an external vendor portal exists, there would be no further action required, as traceability may be reviewed from the vendor portal. However, in a current state scenario, it is recommended that CDAP Management telephone any vendors expected to be submitting documentation to make them aware of a potential temporary delay in review via email.

Initial Resolution Step(s): When email systems are down, CDAP team members should confirm the outage internally (among CDAP resources), and then identify active CDAP records where traceability and/or Form 918 information is expected imminently. As deemed necessary, CDAP Management should contact impacted vendors (i.e. those with a short period of time to submit required traceability) via telephone to notify them of the outage. Additionally, if required, CDAP Management can inform the vendors that they will be granted an additional amnesty period for traceability submission in response to the outage.

5.2.2.3 Automated Communication System

Many potential future-state platforms come equipped with prepackaged automated communication features. These features can be utilized to inform vendors of successful traceability submissions (i.e. without data errors), update vendors on review statuses (e.g. traceability approved or denied) and notify them if there are other issues/questions with their records. In preparation for any potential outages for a future platform, CDAP Management should work with J6 and/or the technical integrator to ensure an administrator account is setup for internal CDAP use. This account will be of paramount importance when it comes to verifying potential outages. In case of an outage, the CDAP team should monitor vendor submissions and revert to manual email notifications when new information is submitted, reviewed, etc. IN preparation for this eventuality, each member of the CDAP Management team should have stored copies of the email templates pre-prepared for each scenario (i.e. vendor information submitted, reviewed, rejected, etc.).

Initial Resolution Step(s): CDAP Management should utilize the administrator account to confirm the system is not functioning properly. This can be done by attempting an action which normally triggers an automated communication (i.e. submit traceability via the vendor portal and check whether a confirmation email is received), or by monitoring communication metrics (to look for unusual inactivity) within the platform if that capability exists within the platform.

5.2.2.4 Workload Management System

Existing CDAP processes rely on functionality within existing DLA business systems to route information and requests via a workload management system and Post Award Requests (PAR). Additionally, future plans for more efficient data collection and review via a digital solution include the implementation of a workflow management system to help facilitate data reviews as external vendors submit information. As such, it is important to the continuity of the CDAP program that workload management is unaffected in the case of a system outage. Should a failure of the workload management system occur, CDAP team members should periodically check the queue of incoming submissions for new records. CDAP resources should also manually assign reviews and temporarily track statuses and review progress manually. When system usage is restored, any status updates or record changes should be transferred to the system of record via upload or other database update.

Initial Resolution Step(s): When the system outage is identified, CDAP should report the outage to the Enterprise Help Desk and communicate the outage within the internal CDAP team. Resources should understand how to manually review incoming data and how to temporarily track (via Word, Excel, etc.) review statuses and new information until the system is restored.

5.2.2.5 Data Storage

While storing data in an enterprise environment has a variety of benefits, this approach is susceptible to potential program delay should an unforeseen disaster temporarily disable access to the system of record. However, to prepare for this situation, DLA J6 has a variety of robust continuity of operations and enterprise system contingency plans in place with DISA and other service providers. As such, it is expected that any disruption to data access would likely not result in data loss, rather would result in a temporary inability to access data until appropriate service levels for restoring service are met. As a contingency for potential database disruption, CDAP Management should periodically (recommended monthly or bi-weekly) download an extract of all ‘open’ data records and reviews. This extract should capture the majority of all active (i.e. in process) reviews depending on periodicity, given that the process typically takes more than a week to complete.

Initial Resolution Step(s): CDAP users should immediately report the inability to access data to the Enterprise Help Desk. The Help Desk should then be able to escalate the issue as necessary and enact the enterprise contingency to restore access and recover data if needed in extreme circumstances.

5.2.2.6 eProcurement (Contracting) System

Although it is only an ancillary aspect of the core CDAP process, system outage of the contracting system of record (eProcurement) can impact the CDAP process. An eProcurement outage would primarily delay contracting, which may render contracting officers unable to produce new awards and/or process Post Award Requests (PAR). The inability to access and read PARs is the primary impact to awards that have already been made. As is the case with enterprise data storage, any outage to the eProcurement system or EBS would be covered under the enterprise continuity of operations and contingency plans. In the unlikely circumstance of an eProcurement outage, CDAP resources should directly contact (via email, Skype, etc.) Procurement or other process area experts in lieu of utilizing PARs.

Initial Resolution Step(s): Although it is unlikely that an eProcurement outage may not be noticed by CDAP users before Procurement users, CDAP users should notify the Enterprise Help Desk immediately if they believe there is an issue with eProcurement and/or Post Award Request functionality. Help Desk resources should be able to confirm the issue and escalate as necessary to restore service and functionality.

5.2.2.7 Individual CDAP User Computer/Email

A more common, but lower impact issue may be computer and/or downtime experienced by single individuals working under the CDAP program. Computer and/or email outages can be caused by a variety of issues (i.e. CAC Card credentials, hardware issues, software updates, etc.), so they are likely to be more common than other issues. When this situation occurs, the CDAP resource affected should notify CDAP leadership and temporarily re-assign review duties if there are any high criticality or time-dependent reviews in-process. Generally, computer and/or email issues are able to be resolved in a timely manner, causing minimal disruption.

Initial Resolution Step(s): Upon identifying a computer and/or email issue, the CDAP resource should contact the Enterprise Help Desk and troubleshoot the issue over the phone. Help Desk resources should be able to determine a root cause and solution but can also escalate the issue if a solution is not found.

5.2.3 Contingency Execution

Members of CDAP should be designated to perform the various roles to effectively carry out the review process in case of need to execute a contingency plan. Responsibilities assigned to roles include management and oversight, traceability reviews, and maintenance of databases. Management and oversight of proper execution of a contingency plan should be designated to a resource as a supervisory role. This role would have the responsibility of ensuring CDAP team members meet predefined milestones, educate and maintain team knowledge of contingency plan procedure, and designate other responsibilities to team members.

Maintenance of applicable databases will be crucial in preventing a delay in traceability review completion. This responsibility includes ensuring integrity and availability of traceability status and documentation as well as the proposed vendor distribution list. Once all processes are defined and roles assigned, further discussions should take place about increasing integrity and availability of data and workflow once Form-918 data capture and storage methods have been solidified.

5.2.4 Digital Traceability Communications Plan

The potential failures outlined by the CDAP Contingency Plan must be communicated to external vendors in order to be effective. A communication plan has been designed to encompass all seven of the potential failures identified. Providing support to external vendors in case of an unplanned outage is essential to maintaining continuity of CDAP's operations. The three key communication mediums identified are (1) vendor-facing portal, (2) outage screens, and (3) Automatic notification e-mails. The following subsections will detail the communication method for each medium.

5.2.4.1 Vendor-Facing Portal

On the vendor-facing portal, contact information for the CDAP office should be readily available for external vendors in case of issues with submission or one of the scenarios identified in the contingency plan. The recommended contact method would be the shared CDAP office email that is currently used to submit documentation. The CDAP office telephone number should also be shared with external vendors in case CDAP email servers are down. Instructions for the alternative submission method recommended in the Contingency Plan should also be made available on the vendor-facing portal.

5.2.4.2 Outage Screens

In case of a system outage, the vendor-facing portal should present alternative contact methods to external vendors. The vendor-facing portal for CDAP users should redirect to a system outage page. The recommended contact method is by phone. The CDAP office phone number should be present so that a vendor could call to move forward in the CDAP process. The contingency plan for a CDAP system outage would be communicated by the CDAP office.

5.2.4.3 Automatic Notification Email

The future state CDAP process would include notification emails to vendors. In multiple steps in the process an email is sent to the vendor notifying them of the status of their award. Within these emails, the contact information for the CDAP office should be made available to ensure vendors working with CDAP always have an alternative contact method. Once a vendor successfully submits a digital Form-918, they will always have CDAPs alternative contact information available. In the case of an either system outage or e-mail server outage, the CDAP office phone number should be made available to vendors.

6.0 Recommended CDAP Enhancements

As outlined in this report, there are many opportunities for improvement within the existing Counterfeit Detection and Avoidance Program. Many of these problems stem from the manual nature of existing processes and can be mitigated by digitizing the data and creating new methods for information sharing. The primary recommendations for enhancing this process are to: (i) collect Form-918 data through a web-based form, (ii) store CDAP data in a shareable enterprise database, and (iii) develop/analyze relevant business intelligence metrics. As this section will discuss further, the implementation of these recommended enhancements will provide benefits to all stakeholders in the CDAP process, both internal and external to DLA.

6.1 Web-Based DLA Land & Maritime Form-918

Through collaboration with the CDAP team at DLA Land & Maritime, it was determined that the manual nature of the existing process results in a high error rate and lengthy review times for traceability documentation. Therefore, it is recommended that a web-based DLA Land & Maritime Form-918 be created for CDAP data collection to incorporate automation, data validation, and improved ease of use. The following sections will detail a prototype Form-918 developed to demonstrate the potential future state appearance and functionality of this type of enhancement.

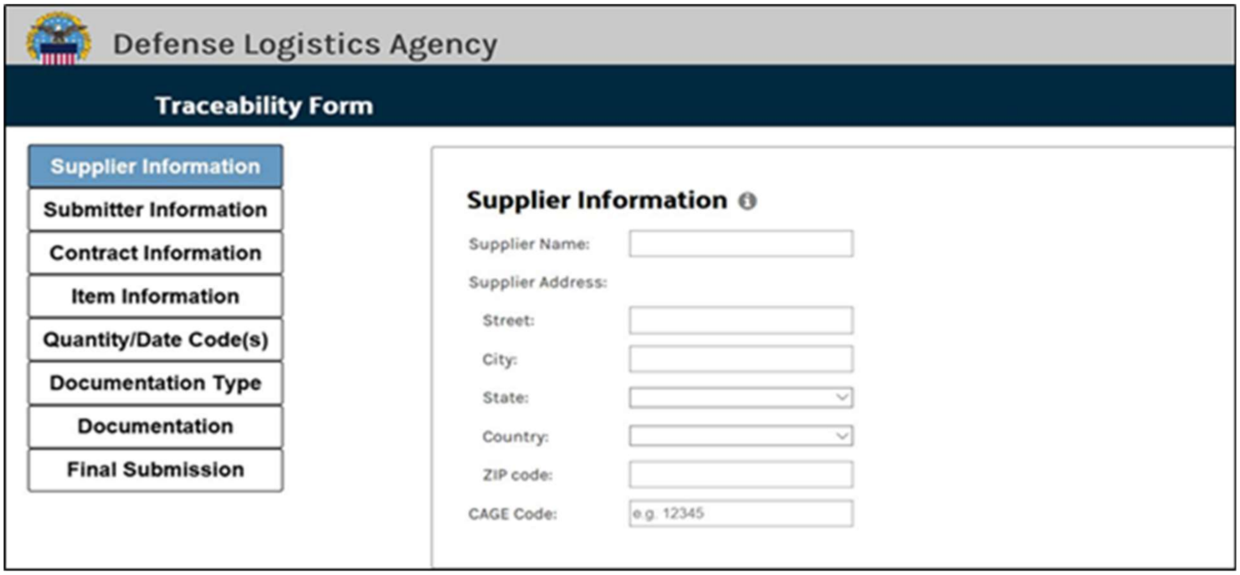
One consideration when developing this Form-918 prototype was the need to maintain existing Form-918 sections and required data elements. This approach ensures that previously collected data is in the same format and external suppliers will not have any new submission requirements. Screenshots of each major section within the prototype form will be shown and described in more detail including:

- **Supplier Information** – General characteristic information about the supplier
- **Submitter Information** – Contact information for the submitter (point of contact)
- **Contract Information** – Information about the contract details
- **Item Information** – Information about the item being procured by DLA
- **Quantity/Date Code(s)** – Production date, lot, and quantity information
- **Documentation Type** – Traceability documentation type
- **Documentation** – Submission of traceability documentation
- **Final Submission** – Review and submission of completed information

Digitizing the collection of CDAP information will provide a variety of benefits which will be discussed in detail within later sections. However, other notable functionality improvements include a quick navigation bar, information buttons (help buttons), drop-down lists, field suggestions (format suggestions), and real-time field validations.

6.1.1 Supplier Information

The first section of Form-918 is meant to collect basic information pertaining to the supplier who has been awarded the Purchase Order. This basic information includes the Supplier Name, Supplier CAGE code, and Supplier Address consisting of Street, City, State, Country, and Zip Code. A screenshot of the prototype view for this section is shown below in Figure 16.



Supplier Information

Supplier Name:

Supplier Address:

Street:

City:

State:

Country:

ZIP code:

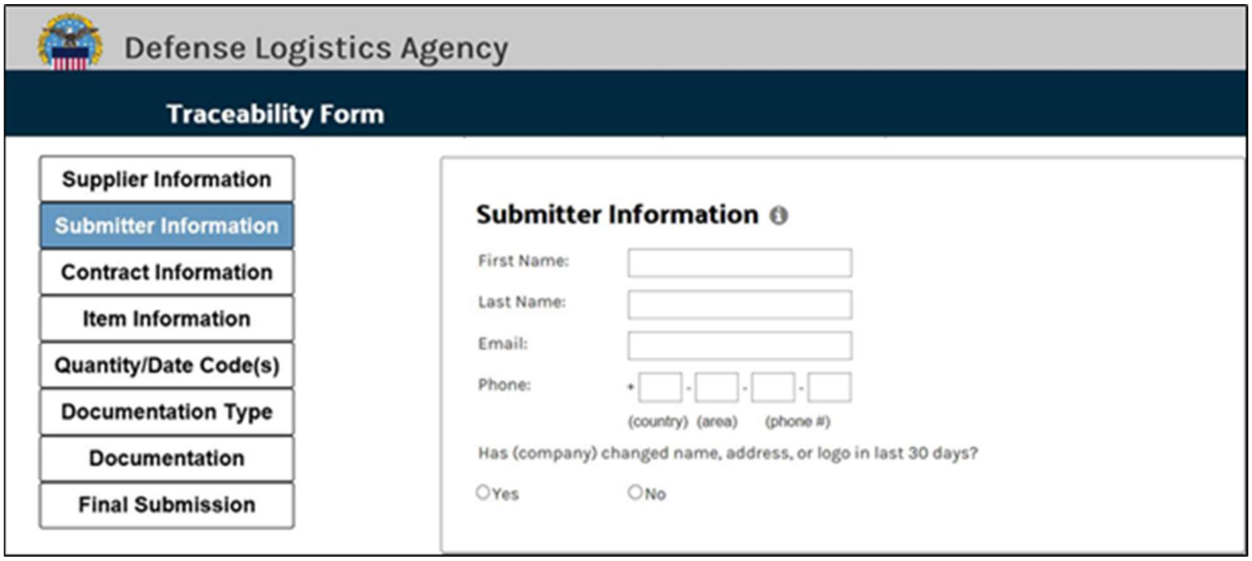
CAGE Code: e.g. 12345

Figure 16. *Supplier Information section of Digital Form-918*

When pressed and/or hovered over, the information button for this section displays the following: "Enter Supplier Name, Address, and CAGE code."

6.1.2 Submitter Information

The second section collects information about the person submitting and responsible for the information on behalf of the supplier and/or acting as a point of contact. This section includes contact information such as First Name, Last Name, Email, and Phone Number. In addition, a new field asks whether the company has changed any of their information (name, address, or logo) in the past month to identify and changes. If the submitter indicates that the company's identity has recently changed, they will be required to give an explanation and upload documents to validate any changes. A screenshot of the prototype view for this section is shown below in Figure 17.



Submitter Information

First Name:

Last Name:

Email:

Phone: + - - -

(country) (area) (phone #)

Has (company) changed name, address, or logo in last 30 days?

○Yes ○No

Figure 17. *Submitter Information section of Digital Form-918*

When pressed and/or hovered over, the information button for this section displays the following: "Enter the Name, Email, and Phone Number of the person submitting this form. If your company has changed their Name, Address, or Logo in the last 30 days please select yes, and upload documentation to verify the changes."

6.1.3 Contract Information

The Contract Information section is very short and simply asks for the awarded Contract Number (Purchase Order Number) and corresponding Contract Line Item Number (CLIN). A screenshot of the prototype view for this section is shown below in Figure 18.

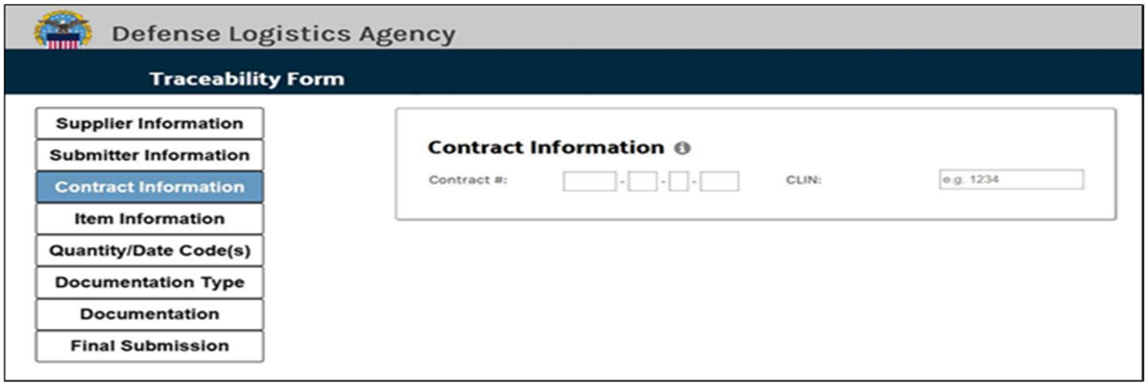


Figure 18. *Contract Information section of Digital Form-918*

When pressed and/or hovered over, the information button for this section displays the following: "Enter the contract number and CLIN as it matches the award information."

6.1.4 Item Information

The item information section collects relevant data about the item being procured and the original component manufacturer. The fields in this section include Item Name, Part Number, FSC, National Item Identification Number (NIIN), Part Manufacturer, and Manufacturer CAGE. A screenshot of the prototype view for this section is shown below in Figure 19.

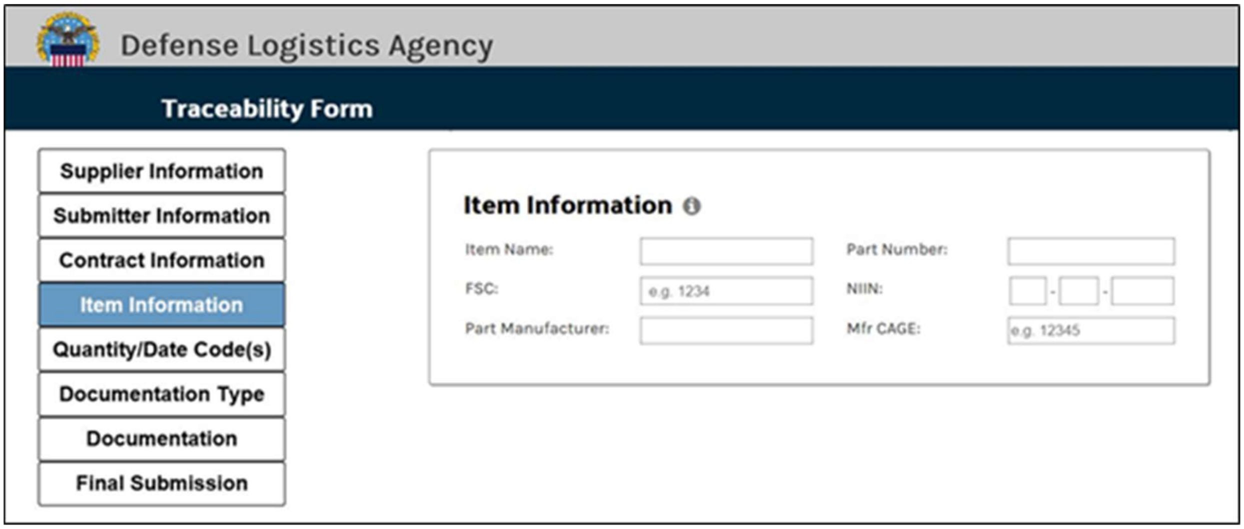


Figure 19. *Item Information section of Digital Form-918*

When pressed and/or hovered over, the information button for this section displays the following: "Enter the name of the Part and its corresponding FSC code, NIIN code, and Part Number. Enter the name of the Part Manufacturer and the Manufacturer's CAGE code."

6.1.5 Quantity / Date Codes

The Quantity / Date Codes section is meant to track the relevant lot information for any components that are being provided. Understanding that there can be many disparate lots provided within a single award, this section has functionality to add extra rows for each additional lot by clicking on a "Add more Quantity / Date Codes" button. Fields within this section include the Lot Date Codes and Quantity from each lot. A screenshot of the prototype view for this section is shown below in Figure 20.

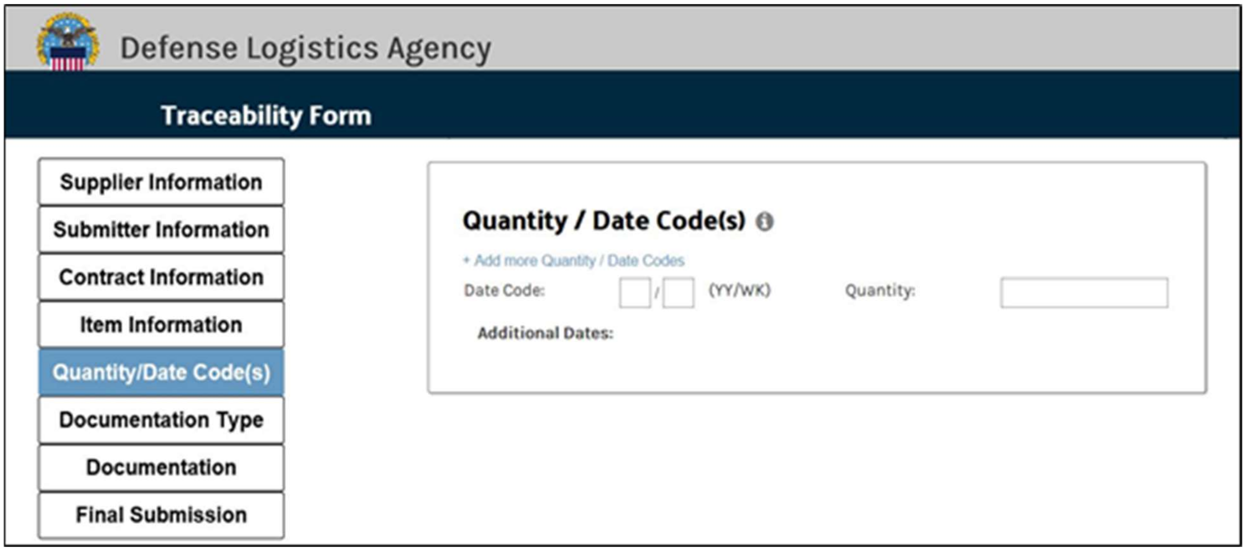
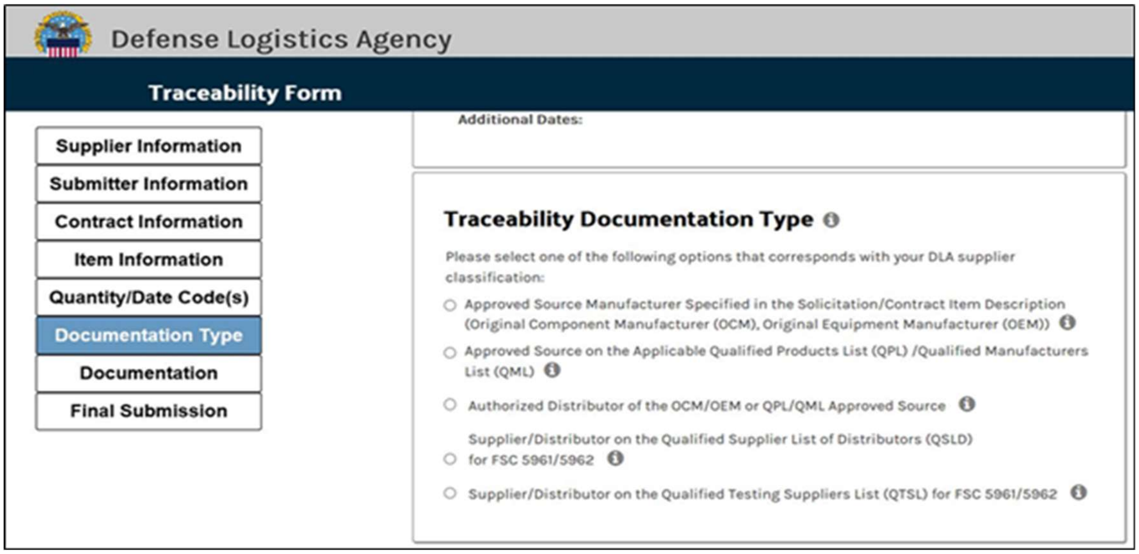


Figure 20. *Quantity/Date Code(s) section of Digital Form-918*

When pressed and/or hovered over the information button for this section displays the following: "Date Code: Input item's date code in YY/WK format. Use the '+ Add multiple date codes and quantities' button to add fields for multiple date codes."

6.1.6 Traceability Documentation Type

The Traceability Documentation Type section consists of five different radio buttons corresponding to different levels of vendor qualification. Suppliers are able to certify themselves as (1) Approved Source Manufacturer Specified in the Solicitation / Contract Item Description (OCM/OEM), (2) Approved Source on the Applicable Qualified Products List (QPL) / Qualified Manufacturers List (QML), (3) Authorized Distributor of the OCM/OEM or QPL/QML Approved Source, (4) Supplier/Distributor on the Qualified Supplier List of Distributors (QSLD) for FSC 5961/5962, or (5) Supplier/Distributor on the Qualified Testing Suppliers List (QTSL) for FSC 5961/5962. A screenshot of the prototype view for this section is shown below in Figure 21.



Traceability Documentation Type

Please select one of the following options that corresponds with your DLA supplier classification:

○ Approved Source Manufacturer Specified in the Solicitation/Contract Item Description (Original Component Manufacturer (OCM), Original Equipment Manufacturer (OEM))

○ Approved Source on the Applicable Qualified Products List (QPL) /Qualified Manufacturers List (QML)

○ Authorized Distributor of the OCM/OEM or QPL/QML Approved Source

○ Supplier/Distributor on the Qualified Supplier List of Distributors (QSLD) for FSC 5961/5962

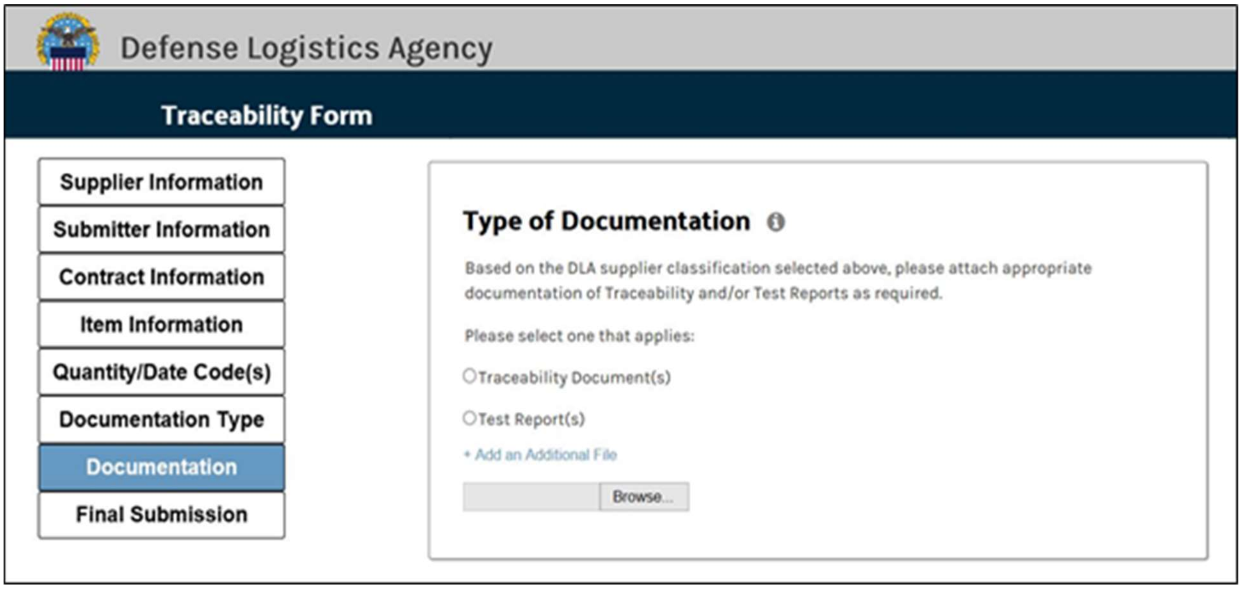
○ Supplier/Distributor on the Qualified Testing Suppliers List (QTSL) for FSC 5961/5962

Figure 21. *Traceability Documentation Type section of Digital Form-918*

When and/or hovered over, the information button for this section displays the following: "Select one option that corresponds with your DLA supplier classification and view the information button for details on what documentation are required."

6.1.7 Type of Documentation

The Type of Documentation section is meant to collect relevant traceability documentation. Based on the supplier's level of qualification as certified in the 'Traceability Documentation Type' section, they can submit Traceability Document(s) and/or a Test Report as applicable. This section also provides functionality for users to attach multiple documents if needed by selecting the 'Add an Additional File' button. A screenshot of the prototype view for this section is shown below in Figure 22.



Type of Documentation

Based on the DLA supplier classification selected above, please attach appropriate documentation of Traceability and/or Test Reports as required.

Please select one that applies:

○ Traceability Document(s)

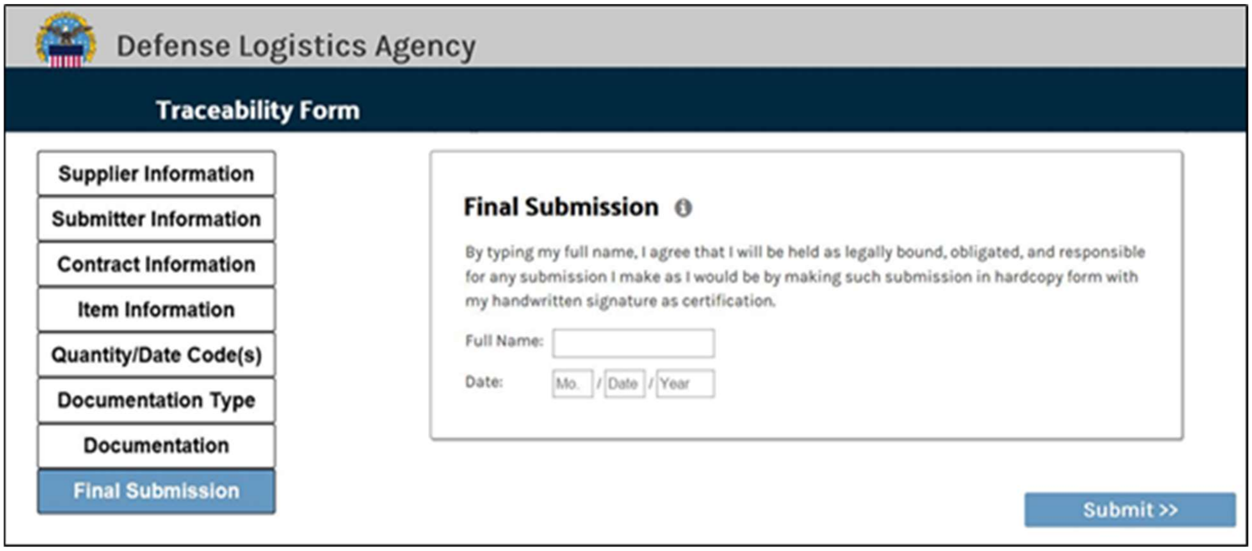
○ Test Report(s)

Figure 22. *Type of Documentation section of Digital Form-918*

When pressed and/or hovered over the information button for this section displays the following: "Please select the type of documentation you're submitting based on your supplier classification and use the 'browse' button to attach the appropriate files."

6.1.8 Final Submission

The Final Submission section is meant to provide the end user with a method for digitally signing and dating the form to certify that all information provided is accurate. This section provides a field for end users to type their Full Name and a date field for them to indicate the Month, Day, and Year. A screenshot of the prototype view for this section is shown below in Figure 23. However, if fields are left incomplete, do not match the hard-coded data validation rules, or has certain types of typographical errors, users will not be able to submit Form-918. Data validations will be detailed in the following section.



Final Submission

By typing my full name, I agree that I will be held as legally bound, obligated, and responsible for any submission I make as I would be by making such submission in hardcopy form with my handwritten signature as certification.

Full Name:

Date: Mo. / Date / Year

Figure 23. *Final Submission section of Digital Form-918*

When pressed and/or hovered over, the information button for this section displays the following: "Enter your full name and todays date and today's date. Click the submit button to submit the form."

6.2 Data Validation Rules

During the current state assessment process, it was discovered that around half of all Form-918 documents submitted as a PDF contained some time of rejection-worthy error, leading to a CDAP rejection. These errors, which are typically simple mistakes like entering information in the wrong field, can cause substantial delays since they require additional correspondence and a new Form-918 submission. It is recommended that DLA include data validation rules within the web-based Form-918 to mitigate the likelihood of such errors occurring.

Data validation rules within the web form can control the types of characters and data inputted into each field and prevent the form from being submitted with data that would be considered invalid. For example, this would prevent a user from entering anything non-numeric in fields such as the Federal Supply Class or National Item Identification Number, both of which are completely numeric when valid.

Table 12 contains recommended data validation 'types' for each field on the form. Alphanumeric fields allow entry of any alphabetic, numeric, or special characters and have no length requirement. Data elements in a required selection must incorporate some type of choice (drop-down, radio button, etc.). Certain fields require specific symbols, character length, or format of characters to be entered, such as email and date code.

Table 12. *Form-918 Data Element Types*

Data Element	Section	Data Type
Street	Supplier Information	Alphanumeric
City	Supplier Information	Character Only
State	Supplier Information	User Selection
Country	Supplier Information	User Selection
Zip Code	Supplier Information	Numeric
CAGE Code	Supplier Information	Alphanumeric
First Name	Submitter Information	Character Only
Last Name	Submitter Information	Character Only
E-Mail	Submitter Information	Alphanumeric
Phone Number	Submitter Information	Numeric
Company Changes	Submitter Information	User Selection
Contract Number	Contract Information	Alphanumeric
Contract Line Item Number (CLIN)	Contract Information	Numeric
Item Name	Item Information	Alphanumeric
Federal Supply Class	Item Information	Numeric
Part Manufacturer	Item Information	Alphanumeric
Part Number	Item Information	Alphanumeric

Data Element	Section	Data Type
Street	Supplier Information	Alphanumeric
City	Supplier Information	Character Only
National Item Identification Number (NIIN)	Item Information	Numeric
Manufacturer CAGE	Item Information	Alphanumeric
Date Code(s)	Quantity / Date Code(s)	Numeric
Quantity	Quantity / Date Code(s)	Numeric
Traceability Documentation Type	Traceability Documentation	User Selection
Type of Documentation	Traceability Documentation	User Selection
Full Name	Final Submission	Character
Date	Final Submission	Date

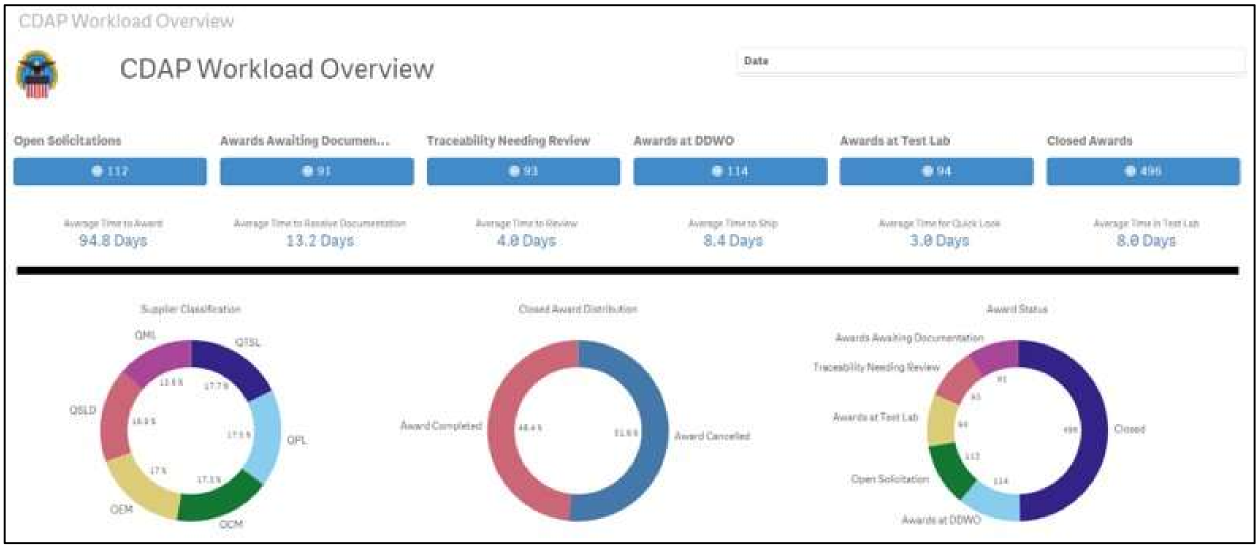
6.3 CDAP Business Intelligence

Business Intelligence (BI) dashboards were developed to give CDAP better insight into its processes and expected workload after digitizing Form-918. The following dashboards provide the CDAP with real-time data to better manage its workload, while also helping glean insights into determining process efficiencies and inefficiencies for continuous improvement. However, please note that because J6 has not yet chosen an enterprise visualization tool, this drafted dashboard was creating using Qlik Sense with the expectation that all views would be ported into DLA's eventual choice, and all data in the following screenshots are notional data elements built off the CDAP catalog.

6.3.1 Workload Overview

The CDAP Workload Overview screen serves as the main landing page for the CDAP BI Dashboard. This screen provides an overview of the status of awards or solicitations in the traceability review process or in its overall pipeline. Each button denotes the amount of awards or reviews each stage of the CDAP review process and can potentially show any underlying problems affecting throughput. Additionally, key metrics are listed to show the average duration at each stage the traceability life cycle, which can be analyzed to further bolster CDAP's business intelligence by predicting day-to-day and future workload.

Please note that the buttons showing the number of awards at each stage were built using a navigation extension and link to drill-down pages. While these extensions may not be compatible with DLA's current systems, it is expected that navigation functionality will be incorporated in future Qlik Sense base updates. Qlik in its base form can still support the drill-downs utilized this dashboard.



CDAP Workload Overview

CDAP Workload Overview

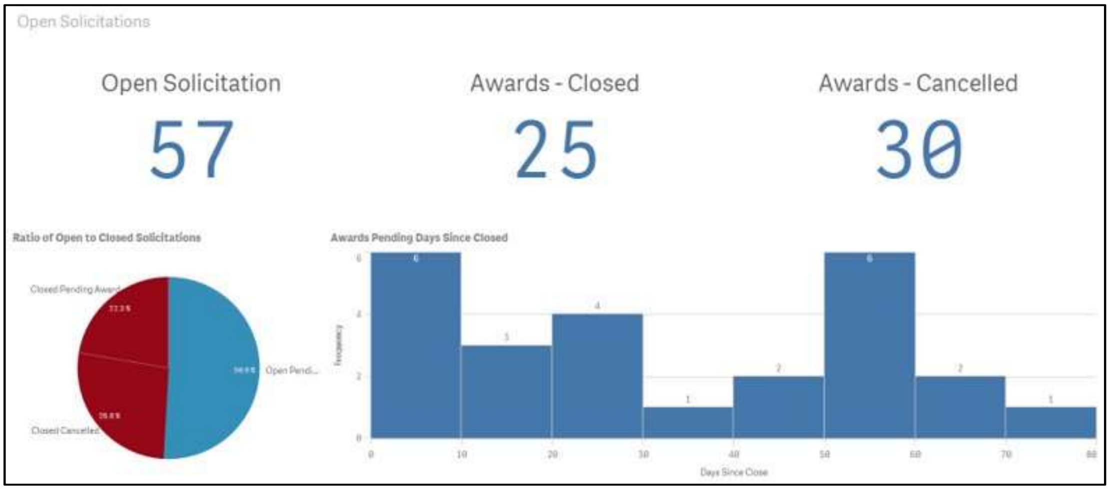
Data

Open Solicitations	Awards Awaiting Documen...	Traceability Needing Review	Awards at DDWO	Awards at Test Lab	Closed Awards
● 112	● 91	● 93	● 114	● 94	● 496
Average Time to Award 94.8 Days	Average Time to Resolve Documentation 13.2 Days	Average Time to Review 4.0 Days	Average Time to Ship 8.4 Days	Average Time for Quick Look 3.0 Days	Average Time in Test Lab 8.0 Days

Figure 24. *CDAP Workload Overview page of CDAP Business Intelligence Dashboard*

6.3.2 Open Solicitations

The Open Solicitations section provides the CDAP team with insight into its expected upcoming workload based upon the number of solicitations open or awaiting award in DLA Internet Bid Board System (DIBBS). For example, the "Awards Pending Days Since Closed" histogram provides a visualization of solicitations that have been closed by procurement (J7); thereby providing the CDAP team with better understanding of when awards will be potentially entering their pipeline. Resulting in better insights into how best to manage workload based upon expected volume.



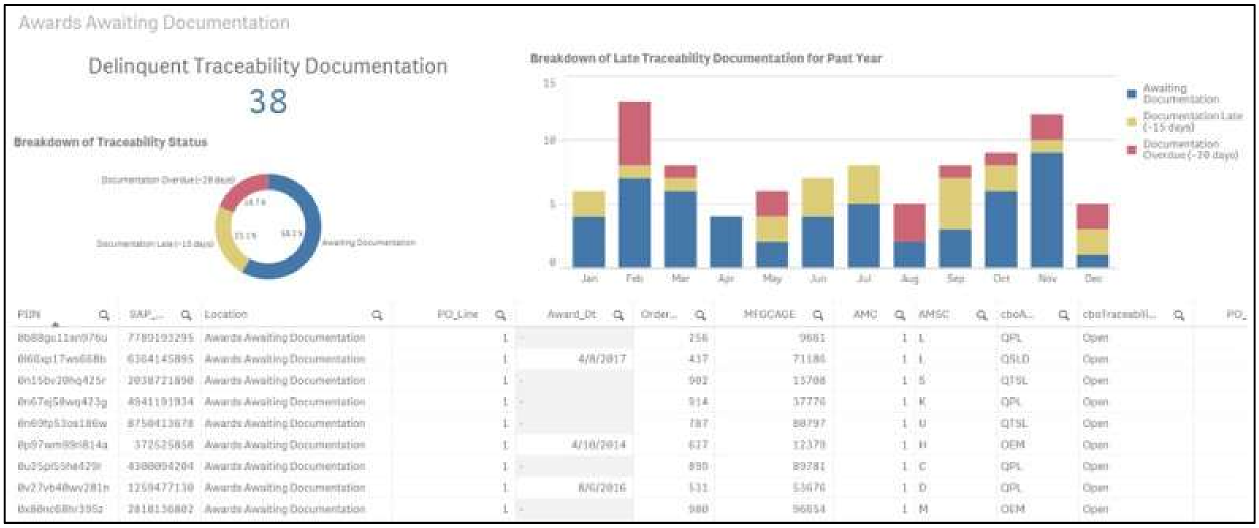
Open Solicitations

Open Solicitation	Awards - Closed	Awards - Cancelled
57	25	30

Figure 25. *Open Solicitations page of CDAP Business Intelligence Dashboard*

6.3.3 Awards Awaiting Documentation

The Awards Awaiting Documentation dashboard denotes how many reviews still require traceability documentation that are either almost due or delinquent. This allows the CDAP team to better prioritize notifying or corresponding with vendors to ensure that the documentation is sent, so that it can be reviewed, and the materials can be delivered to DLA in a timely manner. For example, “Breakdown of Late Traceability Documentation” stacked bar chart allows CDAP to track vendor submission timeliness and is denoted by month; enabling CDAP to predict when documentation may be arriving later than average based on the time of the year.

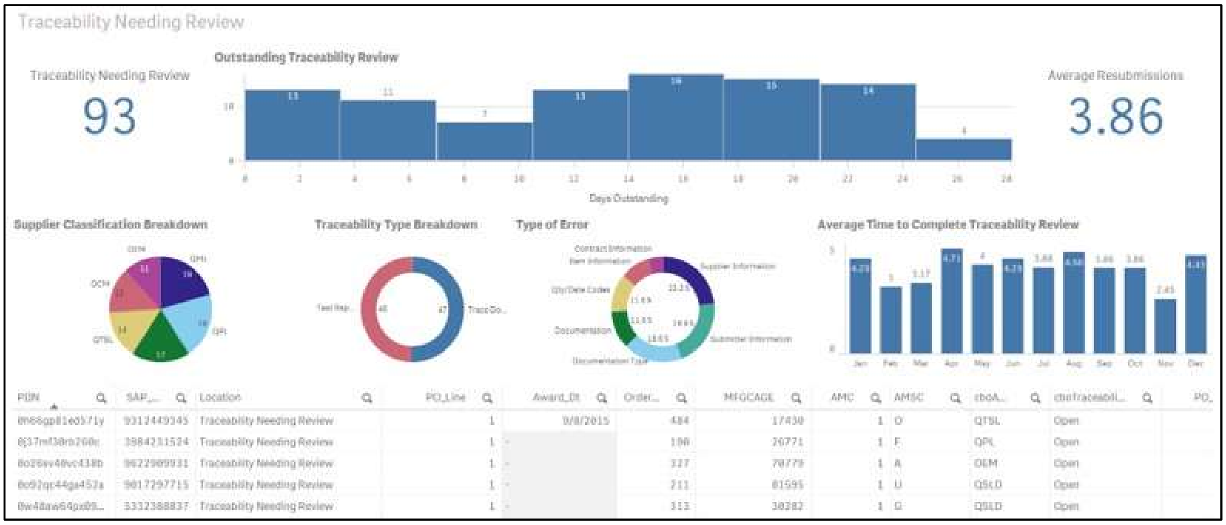

Awards Awaiting Documentation
Delinquent Traceability Documentation
38
Breakdown of Traceability Status
Documentation Overdue (~28 days)
18.7%
Documentation Late (~15 days)
25.1%
58.1%
Awaiting Documentation
Breakdown of Late Traceability Documentation for Past Year
15
10
5
0
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Awaiting Documentation
Documentation Late (~15 days)
Documentation Overdue (~28 days)

PIIN	SAP_...	Location	PO_Line	Award_Dt	Order...	MFGCAGE	AMC	AMSC	cboA...	cboTraceabili...	PO_
0b88gu11an976u	7789193295	Awards Awaiting Documentation	1	-	256	9681	1	L	QPL	Open	
0i60xp17ws668b	6384145895	Awards Awaiting Documentation	1	4/8/2017	437	71186	1	I	QSLD	Open	
0n15bv20hq425r	2038721898	Awards Awaiting Documentation	1	-	902	13708	1	S	QTSL	Open	
0n67ej58wq473g	4941191934	Awards Awaiting Documentation	1	-	914	37776	1	K	QPL	Open	
0n69tp53os186w	8758413678	Awards Awaiting Documentation	1	-	787	88797	1	U	QTSL	Open	
0p97wm89n814a	372525858	Awards Awaiting Documentation	1	4/10/2014	617	12378	1	H	OEM	Open	
0u25pt55he429r	4388894204	Awards Awaiting Documentation	1	-	850	89781	1	C	QPL	Open	
0v27vb48wv281n	1259477130	Awards Awaiting Documentation	1	8/6/2016	531	53676	1	D	QPL	Open	
0x88uc68hr395z	2818136802	Awards Awaiting Documentation	1	-	980	96854	1	M	OEM	Open	

Figure 26. *Awards Awaiting Documentation page of CDAP Business Intelligence Dashboard*

6.3.4 Traceability Needing Review

The Traceability Needing Review dashboard provides visualizations and drill-downs into CDAP’s current workload, allowing for a comprehensive understanding of each status of every instance throughout the review process. The CDAP team can interact with these visualizations to quickly glean the how many reviews are still outstanding, where an instance is in the review process, and the type and classification breakdown of review. As such, the CDAP team will not only be able determine the status of a review but can also determine areas of success and improvement of the web-based Form-918; given that the average resubmission's metric and the most prevalent types of error causing resubmissions are also captured in this dashboard.

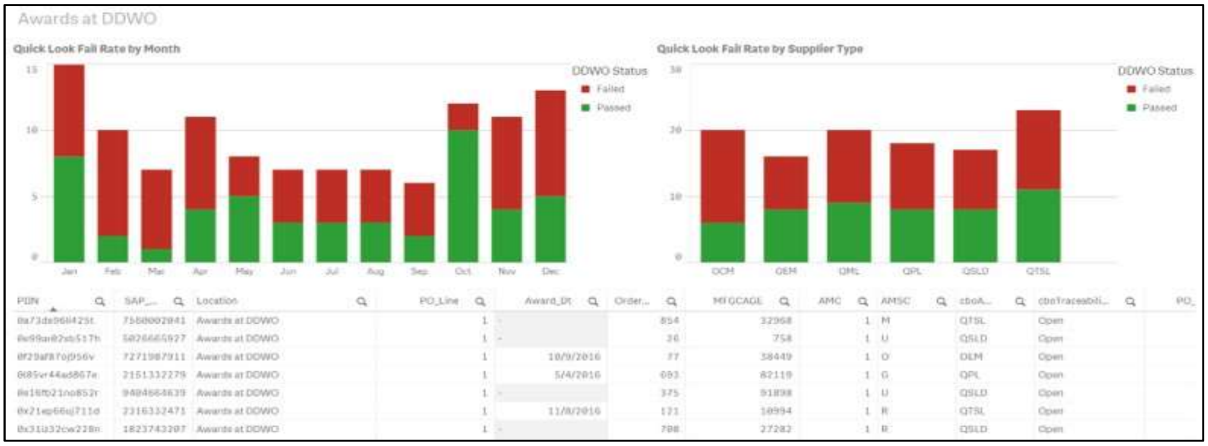


PIIN	SAP_...	Location	PO_Line	Award_Dt	Order...	MFGCAGE	AMC	AMSC	cboA...	cboTraceabili...	PO_
0n86gp81ed571y	9312449345	Traceability Needing Review	1	9/8/2015	484	17430	1	O	QTSL	Open	
0j37mf38rb260c	3984231524	Traceability Needing Review	1	-	198	26771	1	F	QPL	Open	
0o26vv46vc438b	9622989931	Traceability Needing Review	1	-	327	78779	1	A	OEM	Open	
0o92qc44ga457a	9017297715	Traceability Needing Review	1	-	211	81595	1	U	QSLD	Open	
0w48aw64px09...	3332388837	Traceability Needing Review	1	-	313	38282	1	G	QSLD	Open	

Figure 27. *Traceability Needing Review page of CDAP Business Intelligence Dashboard*

6.3.5 Awards at DDWO

The Awards at DDWO provides insights into a vendor's ability to correctly ship material up to DLA's standards. Specifically, the "Quick Look Fail Rate by Supplier Type" stacked bar graph provides data into which supplier classes has meet or fail DLA's standards when shipping material. This allows for a better understanding of the sourcing – by supply type – and its impact within DLA's supply chain.

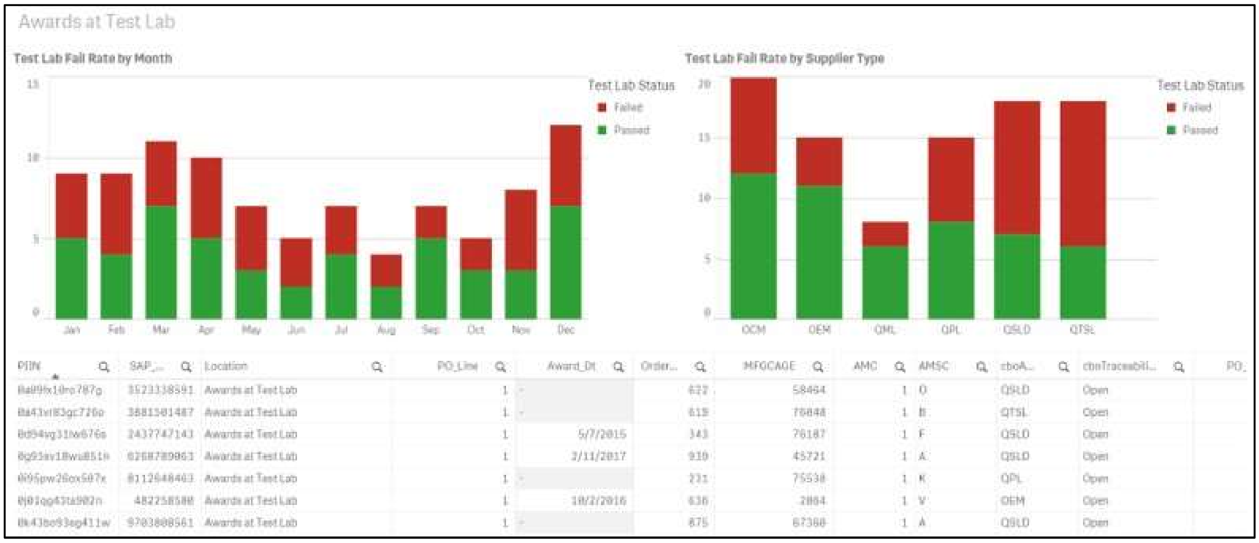


PIIN	SAP_...	Location	PO_Line	Award_Dt	Order...	MFGCAGE	AMC	AMSC	cboA...	cboTraceabili...	PO_
0a73de96li425t	7568002841	Awards at DDWO	1	-	854	32968	1	M	QTSL	Open	
0e99ar82sb517h	5026665927	Awards at DDWO	1	-	26	758	1	U	QSLD	Open	
0f29af87oj956v	7271987911	Awards at DDWO	1	10/9/2016	77	38449	1	O	OEM	Open	
0i85vr44ad867e	2151332279	Awards at DDWO	1	5/4/2016	093	82119	1	G	QPL	Open	
0e16fb21no852r	9484664639	Awards at DDWO	1	-	375	91898	1	U	QSLD	Open	
0x21ep66uj711d	2316332471	Awards at DDWO	1	11/8/2016	171	10994	1	R	QTSL	Open	
0x31u32cw228n	1823743207	Awards at DDWO	1	-	708	27282	1	R	QSLD	Open	

Figure 28. *Awards at DDWO page of CDAP Business Intelligence Dashboard*

6.3.6 Awards at Test Lab

The Awards at Test Lab dashboard provides further insight into visual inspection pass/fail rate for material received by the Test Lab. Here, the pass/fail rate accuracy by supplier type is denoted to help guide business intelligence in decision making for procurement and CDAP scrutiny.

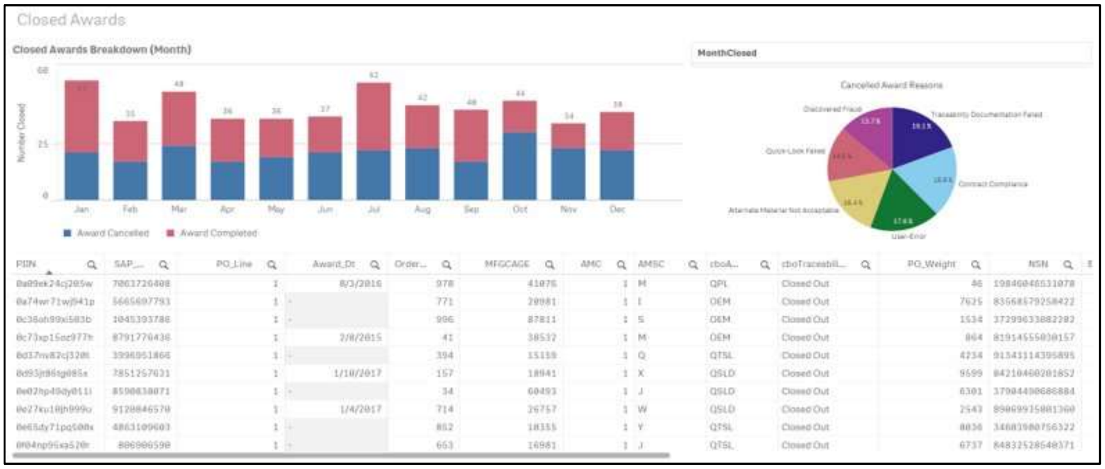


PIIN	SAP_...	Location	PO_Line	Award_Dt	Order...	MFGCAGE	AMC	AMSC	cboA...	cboTraceabili...	PO_
0a89hx10ro787g	3523338591	Awards at Test Lab	1	-	622	58464	1	O	QSLD	Open	
0a43vi83gc726o	3881501487	Awards at Test Lab	1	-	615	76848	1	B	QTSL	Open	
0d94vg31iw676s	2437747143	Awards at Test Lab	1	5/7/2015	343	76187	1	F	QSLD	Open	
0g93av18wu851h	6268789863	Awards at Test Lab	1	2/11/2017	939	45721	1	A	QSLD	Open	
0i95pw26ox587x	8112648463	Awards at Test Lab	1	-	231	75538	1	K	QPL	Open	
0j01qg43ta982n	482258588	Awards at Test Lab	1	10/2/2016	636	2884	1	V	OEM	Open	
0k43bo93ag411w	9703808561	Awards at Test Lab	1	-	875	67388	1	A	QSLD	Open	

Figure 29. *Awards at Test Lab page of CDAP Business Intelligence Dashboard*

6.3.7 CDAP Completed Awards

The CDAP Completed Awards section allows for both the CDAP team and DLA leadership to review the overall performance closing awards and gauge how successful CDAP is in completing the traceability review process. Further analysis can be performed using the "Cancelled Award Reasons" pie chart, which provides detailed insight into why awards were cancelled and can be used by CDAP as a success metric for digital Form-918's ability to reduce user submission errors.



PIIN	SAP_...	PO_Line	Award_Dt	Order...	MFGCAGE	AMC	AMSC	cboA...	cboTraceabil...	PO_Weight	NSN
0a09ek24cj205w	7063726408	1	8/3/2016	978	41076	1	M	QPL	Closed Out	46	1984604653 1078
0a74wr71wj941p	5665697793	1	-	771	20981	1	I	OEM	Closed Out	7625	8356857925 8422
0c38oh99xi583b	1045393788	1	-	996	87811	1	S	OEM	Closed Out	1534	3729963388 2283
0c73xp15oz977h	8791770436	1	2/8/2015	41	38532	1	M	OEM	Closed Out	864	8191455503 0157
0d17mv82cj320l	3998051866	1	-	394	15118	1	Q	QTSL	Closed Out	4234	9154111439 5895
0d93jr86tg085x	7851257631	1	1/10/2017	157	18941	1	X	QSLD	Closed Out	9599	8421046020 1852
0e02hp49dy011i	8590838071	1	-	34	60493	1	J	QSLD	Closed Out	6301	3790449068 8884
0e27ku18jh999u	9128846570	1	1/4/2017	714	26757	1	W	QSLD	Closed Out	2543	8906991580 1360
0e65dy71pq508x	4863109603	1	-	852	18355	1	Y	QTSL	Closed Out	8036	3468398075 6322
0f04np95xa520r	886986598	1	-	663	16981	1	J	QTSL	Closed Out	6737	8483252854 0371

Figure 30. *CDAP Completed Awards page of CDAP Business Intelligence Dashboard*

6.4 Enterprise Data Storage

The CDAP process is highly collaborative and is supported by three different internal stakeholder groups as outlined above. The existing collection of CDAP related information in the CDAP Catalog is a temporary solution for a larger data-sharing and collaboration problem. To help enable more efficient, accurate, and timely data sharing, it is recommended that the CDAP Catalog data (and any other relevant business information) be integrated with DLA's enterprise data systems, namely the Enterprise Data Warehouse (EDW). Integrating CDAP data into EDW will create access for all DLA stakeholders to the data in real time, and would enhance visibility across the enterprise, opening opportunities to improve CDAP and DLA business intelligence.

Given that the CDAP's data is currently stored locally on a shared drive, which is prone to system failure and loss of data, should user error occur, it may be impossible to retrieve the data. Additionally, locally stored files are also prone to user error and are rarely archived or backed up when compared to an external server or cloud database. Therefore, to ensure the integrity and security of data, it is recommended that the CDAP should move away from local storage of data to an enterprise wide data structure such as EDW or another viable database source.

6.5 Summary of Expected Benefits

The expected benefits of implementing a digital Form-918 will allow CDAP to meet the growing demand of parts requiring traceability review. The expected benefits of implementing the digital Form-918 will result in the following outcomes:

- Reduction of manually rejected Form-918 submissions over time
- Overall reduction in number of manual actions required per traceability submission
- Increased knowledge of supplier relationships
- Increased throughput capacity of traceability reviews

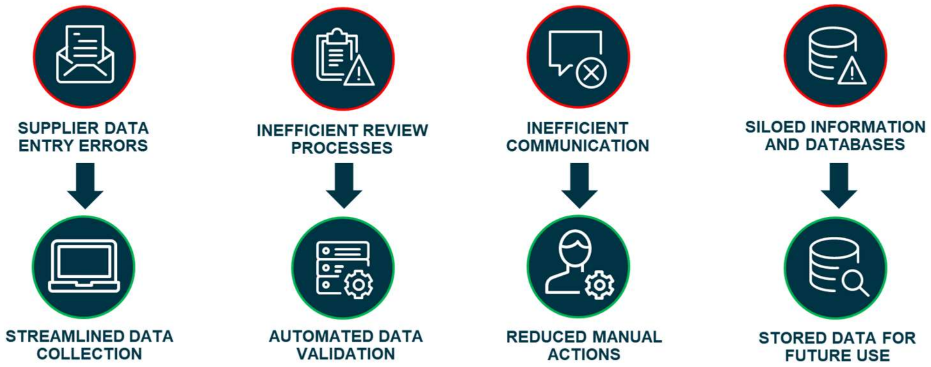

SUPPLIER DATA ENTRY ERRORS
INEFFICIENT REVIEW PROCESSES
INEFFICIENT COMMUNICATION
SILOED INFORMATION AND DATABASES
STREAMLINED DATA COLLECTION
AUTOMATED DATA VALIDATION
REDUCED MANUAL ACTIONS
STORED DATA FOR FUTURE USE

Figure 31. *Current State Issues and Future State Results*

These benefit fit will address CDAP's digital traceability program needs with immediate and longer-term impact that increase usability, review, and overall process of traceability review.

6.5.1 Reduced Error Rate

The addition of built in controls and data validation into digital Form-918 will benefit CDAP by capturing most errors prior to submission. As previously mentioned, vendors have an approximately 50% error rate when submitting the existing Form-918 and data validation rules will help narrow the areas where they need to spend the most time reviewing. Since the built-in controls provide guidance and restrictions to data entry, reducing vendors error rate and potential need for resubmission. For example, when a vendor attempts to submit digital Form-918 with information that does not match the data validation rules, the digital form will highlight incorrect fields, indicating the need for correction prior to submission.

6.5.2 Reduction in Manual Actions

The digital Form-918 will have capabilities for analytics and cross validation. The data entered into fields will be checked against DLA databases, reducing the need for a manual comparison. An example of this benefit is automatically validating that the supplier is qualified by cross-checking the already established Qualified Suppliers List of Distributors (QSLD), QML/QPL, and Qualified Testing Suppliers List (QTSL). This online platform enables CDAP to automatically capture the data submitted in Form-918 and eliminates the need for manual data entry while mitigating potential user-error.

6.5.3 Increased Knowledge of Supplier Relationships

The digital Form-918 will be integrated with DLA's systems. Through integration, DLA will benefit from enterprise access to CDAP's data. The data can benefit DLA across its enterprise for a variety of uses, such as understanding vendor relationships. DLA would be able to utilize CDAP's data to gain a better understanding of the business relationships between vendors. This can also tie back into other CDAP actives, such as, Vendor Network Mapping Capability (VNMC), where through the web-based Form-918 a better understanding of supplier relationships will assist DLA in identifying high-risk supply networks.

6.5.4 Increased Throughput Capacity

The replacement of the paper-based Form-918 with a web-based form, will lead to increased throughput capacity by allowing CDAP to expand traceability reviews to more FSCs. As the image below shows, analytics and data validation will lead to reduced review time by eliminating much of the need for manual review, thereby reducing waste. Waste in resource time is derived from the amount of manual actions required to complete traceability reviews, and with this reduced review time and increased throughput ultimately result in an enhanced and more efficient traceability review process.

The future state diagram also shows the enhanced CDAP traceability review processes in orange. The first enhancement is the vendor submitting Form-918 digitally aided with data validation. Through data validation the error rate of Form-918 submissions will decrease, resulting in an increase of resources' available time. The built-in analytics will aid the CDAP team during its traceability review. By instantly cross checking the data entered the form, the CDAP team will be more readily able to identify discrepancies. Once the Form-918 and traceability documentation are deemed acceptable, the CDAP team can digitally sign completed Form-918, releasing the approval-to-ship notice to the vendor.

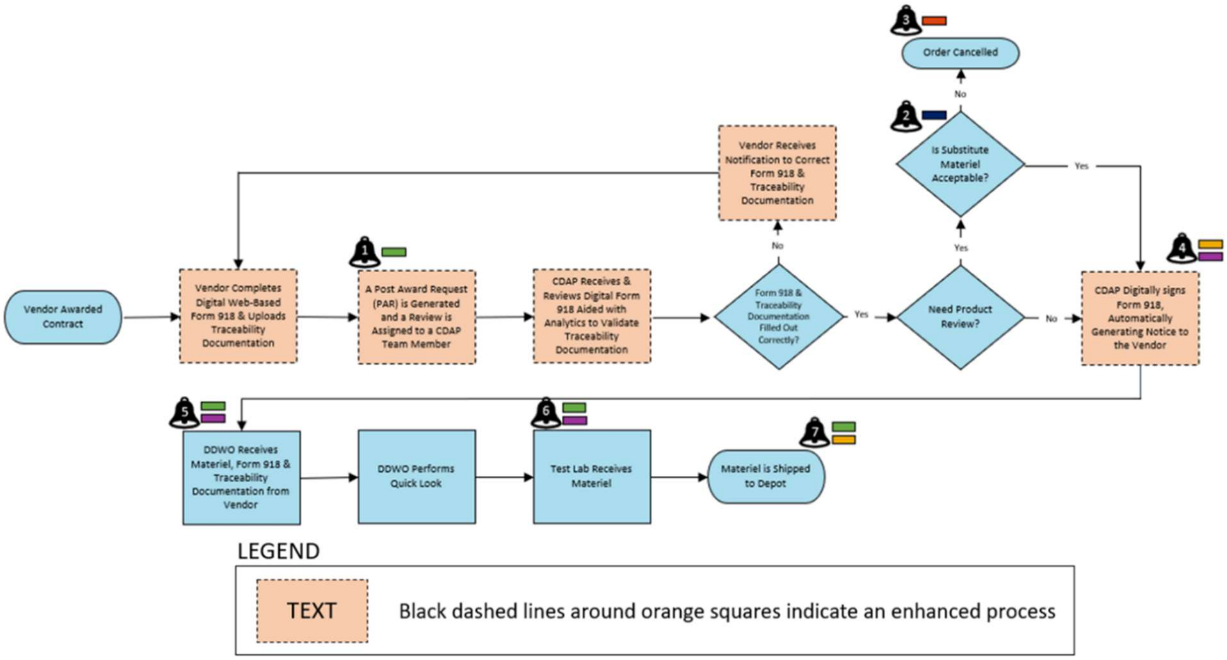
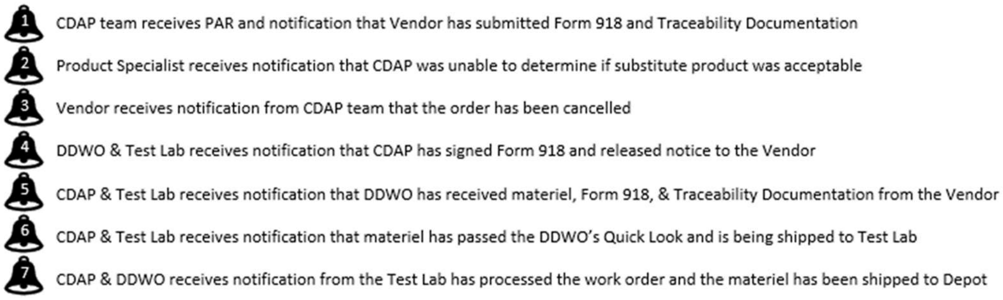

3
Order Cancelled
No
2
Is Substitute Materiel Acceptable?
Yes
Vendor Receives Notification to Correct Form 918 & Traceability Documentation
No
Yes
1
4
Vendor Awarded Contract
Vendor Completes Digital Web-Based Form 918 & Uploads Traceability Documentation
A Post Award Request (PAR) is Generated and a Review is Assigned to a CDAP Team Member
CDAP Receives & Reviews Digital Form 918 Aided with Analytics to Validate Traceability Documentation
Form 918 & Traceability Documentation Filled Out Correctly?
Yes
Need Product Review?
No
CDAP Digitally signs Form 918, Automatically Generating Notice to the Vendor
5
6
7
DDWO Receives Materiel, Form 918 & Traceability Documentation from Vendor
DDWO Performs Quick Look
Test Lab Receives Materiel
Materiel is Shipped to Depot
LEGEND
TEXT
Black dashed lines around orange squares indicate an enhanced process

Figure 32. *Proposed simplified future-state CDAP traceability Process*

Processes regarding product review, DDWO, and Test lab review are inherently unchanged, but are enhanced through data availability and transparency of the review process between stakeholders. The increased transparency of CDAP's data to stakeholders in the traceability process will provide a variety of benefits enterprise-wide. The DDWO and test lab will be able to prioritize and better manage its resources. Utilizing resources more efficiently will reduce any bottlenecks in the process and increase overall workload capacity.

6.5.5 Enabled Push Notifications

To further streamline insights and create process improvements in the CDAP traceability review process, the following notifications are recommended to alert different CDAP stakeholders of a status change that has moved into their respective workflow.



1 CDAP team receives PAR and notification that Vendor has submitted Form 918 and Traceability Documentation

2 Product Specialist receives notification that CDAP was unable to determine if substitute product was acceptable

3 Vendor receives notification from CDAP team that the order has been cancelled

4 DDWO & Test Lab receives notification that CDAP has signed Form 918 and released notice to the Vendor

5 CDAP & Test Lab receives notification that DDWO has received materiel, Form 918, & Traceability Documentation from the Vendor

6 CDAP & Test Lab receives notification that materiel has passed the DDWO's Quick Look and is being shipped to Test Lab

7 CDAP & DDWO receives notification from the Test Lab has processed the work order and the materiel has been shipped to Depot

Figure 33. *Proposed notifications for transitions in traceability review process*

7.0 Trade Security Control (TSC)

7.1 TSC Introduction

The initial phase of the Digital Traceability project included an analysis of the Counterfeit Detection and Avoidance Program (CDAP) and recommendation of enhanced processes and procedures to digitize what is now a very manually intensive process. Upon developing the framework for implementing a web-based data collection form, it was discovered that a related program was experiencing similar issues. As such, the Digital Traceability project was extended to analyze the Trade Security Control (TSC) program and apply similar techniques to provide recommended business requirements. Although the TSC program would also benefit from a web-based form for collecting external data, the data being collected contains sensitive personally identifiable information (PII) and would require a heightened level of security versus the CDAP design. The following sections briefly describe the program, recommended future state processes, and ultimately recommended business requirements for collecting DD Form 1822 information via a web-based form.

7.2 TSC Background[1]

Trade Security Controls (TSC) was implemented to control the transfer of U.S. Munitions List (USML) and Commerce Control List (CCL) personal property to parties outside of DoD control. The Trade Security Control Administration Office (TSCAO) administers the controls enacted by the DoD Directive 2030.8, "Trade Security Controls on DoD Excess and Surplus Personal Property" under the Office of the Inspector General (OIG). The responsibilities of TSC include the demilitarization of defense goods, assessing the eligibility of individuals to possess DoD property, and limiting access to defense property and technical data. The illegal transfer of USML/CCL personal property poses U.S military and security risks. DoD property can contain written or electronic technical data that can be used by foreign adversaries to gain insight into U.S. military technology.

Individuals and entities requesting access to controlled DoD property must submit DLA Form 1822 and be granted End-Use Certificates (EUC) before possession of controlled property. Individuals and entities submitting Form 1822 must disclose why they are requesting possession of DoD property and what they will do with it once it is in their possession. The TSCAO administers strict guidelines on what can and cannot be done with controlled property to mitigate risks associated with controlled defense property. After an EUC has been granted, the TSC continues to monitor the use of controlled property to identify and prevent illegal transfer of defense goods to those whose interests are averse to the U.S.

[1] **Source: https://fas.org/irp/doddir/dod/i2030_08.pdf**

7.3 TSC DD Form 1822

A key component of the Trade Security Control process is the completion of DD Form 1822 by the external user. This form, which ultimately becomes an End-Use Certificate when completed and granted, plays a central role in the certification and tracking process. As such, the digitization of this form and the introduction of field-level validations will be key to reducing the error and return rates. The fields appearing on DD Form 1822 and general field-level characteristics are displayed in Table 13 below.

Table 13. *DD Form 1822 Data Element Types*

Data Element	Section	Data Type
This statement is submitted in connection with:	Header	User Selection / Free Text
Line Item Number / Commodity / Technical Data Request	Header	Numeric
Name	Header	Character Only
SSN / Alien Card No. / Country ID	Header	Numeric
Date of Birth	Header	Date
Place of Birth	Header	Character Only
Telephone Number	Header	Numeric
Mailing Address	Header	Alphanumeric
Physical Address	Header	Alphanumeric
Type of Firm	General Information	User Selection / Free Text
Nature of End User's Business	General Information	Character Only
Nature of Principal's Business	General Information	Character Only
Firm's ID / Federal Tax Number	General Information	Numeric
Business / Corporation Headquarters: Name	General Information	Character Only
Business / Corporation Headquarters: Address	General Information	Alphanumeric
Branch Office: Name	General Information	Character Only
Branch Office: Address	General Information	Alphanumeric
If this is a negotiated exchange, identify the property being exchanged:	End Use / User Information	Character Only
Purpose. The property referred to in above IFB/Offer or DD2345 number will be utilized for the following:	End Use / User Information	User Selection / Free Text
A. Retention for the following specific use (see note):	End Use / User Information	User Selection / Free Text
B. Resold or retransferred in the form received for the following use (see note):	End Use / User Information	User Selection / Free Text
C. The property will not be sold or otherwise transferred or disposed of for use outside of the United States or to non-	End Use / User Information	User Selection

Data Element	Section	Data Type
D. The property may be exported or re-exported in the form received to the following country/countries:	End Use / User Information	User Selection / Free Text
E. Resale after following alteration (description of final production: (fill), in (Country/Countries): (fill), and distribution in (Country/Countries): (fill)	End Use / User Information	User Selection / Free Text
F. If sold or retransferred, name, address, and telephone number of sub-purchaser(s)/sub-contractor(s):	End Use / User Information	User Selection / Free Text
G. The customers are unknown at this time. If required by the contract/transfer document, I will obtain prior written approval for the resale of any of the property covered by this contract.	End Use / User Information	User Selection
Additional Information	End Use / User Information	Free Text
The person signing this DLA Form 1822 is:	Certification Statement	User Selection / Free Text
A. Name	Certification Statement	Character Only
B. Signature	Certification Statement	Digital Signature
C. Date Signed	Certification Statement	Date

For portions of the form such as most of Section II. End Use / User Information and Section IV. Certification Statement, the user will have the option to select one of several options (via checkbox), which may or may not require additional free text to be completed. In addition to field-level validations (which will disallow submission if 'data types' are not adhered to), the web-based form will also require completion of all required fields, which may change based on selections.

7.4 TSC Current State Processes

After an external user completes a DD Form 1822 and submits it for Trade Security Control review, a series of internal processes are triggered. The form is first reviewed for 'quality control' to ensure that the information is complete and no obviously erroneous data is present (e.g. putting Company Name in the CAGE Code field). While error rates are not currently tracked, TSC representatives have estimated this initial rejection rate at approximately thirty to forty percent. Once an 'administratively correct' form passes this check, the data is manually entered into the DLA Criminal Incident Reporting System (DCIRS) and any additional documentation is manually scanned, uploaded, and attached to the record. Next, a series of nine external reviews are completed to check for derogatory information and the results are documented within DCIRS. Finally, a Treasury Enforcement Communication System (TECS) report is prepared and sent to Immigration and Customs Enforcement (ICE) for a final review of potential outstanding negative information. When the TECS results are returned to DLA, the information is manually added to the DCIRS file. In total, these highly manual processes require approximately ninety minutes of manual work per

EUC under best case circumstances. As a result, more than 1,700 EUCs remain pending in a backlog as they are worked.

In an effort to better understand the existing Trade Security Controls process and visually depict where improvements could be made, flow charts depicting the typical flow of information within the program were examined. While available process maps may be slightly out of date, they provide general context for the program and how efficiencies can be gained by moving to a more automated process. Figure 34 below shows the initial steps of the TSC process.

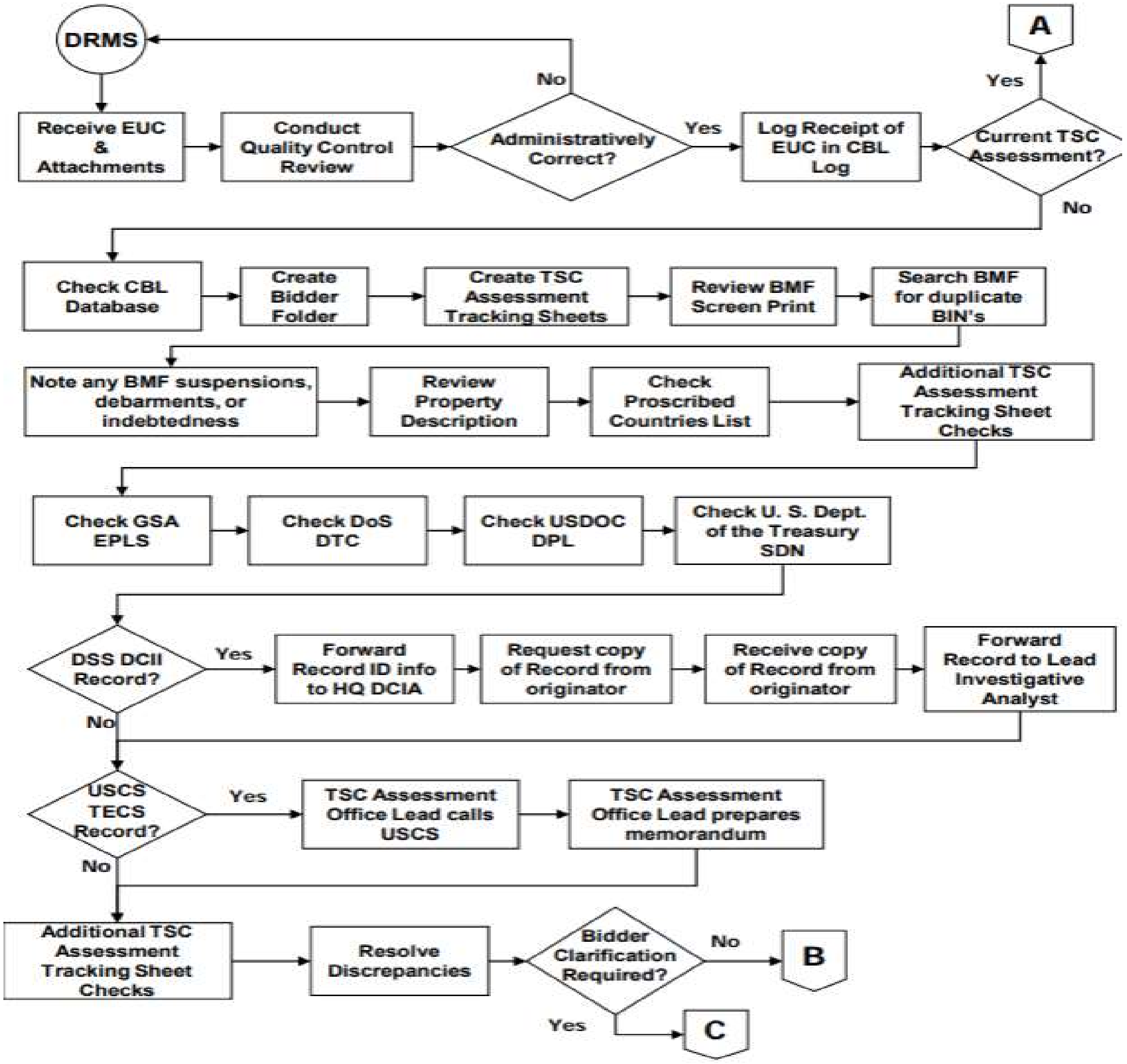

DRMS
No
Receive EUC & Attachments
Conduct Quality Control Review
Administratively Correct?
Yes
Log Receipt of EUC in CBL Log
Current TSC Assessment?
Yes
A
No
Check CBL Database
Create Bidder Folder
Create TSC Assessment Tracking Sheets
Review BMF Screen Print
Search BMF for duplicate BIN's
Note any BMF suspensions, debarments, or indebtedness
Review Property Description
Check Proscribed Countries List
Additional TSC Assessment Tracking Sheet Checks
Check GSA EPLS
Check DoS DTC
Check USDOC DPL
Check U. S. Dept. of the Treasury SDN
DSS DCII Record?
Yes
Forward Record ID info to HQ DCIA
Request copy of Record from originator
Receive copy of Record from originator
Forward Record to Lead Investigative Analyst
No
USCS TECS Record?
Yes
TSC Assessment Office Lead calls USCS
TSC Assessment Office Lead prepares memorandum
No
Additional TSC Assessment Tracking Sheet Checks
Resolve Discrepancies
Bidder Clarification Required?
No
B
Yes
C

Figure 34. *Part One of Trade Security Control Process*

Although the initial steps of receiving an End-Use Certificate (EUC) and checking it for errors only consist of a small portion of the process, they are responsible for the majority of the errors found during the process and resultant delays. Consistent with issues uncovered with the CDAP process, the majority of end user submissions of EUC have to be returned and resubmitted due to incorrect, incomplete, or misplaced information. Beyond the initial 'completeness' checks, the TSC process starts with a review of local databases and single external-site checks to review any potential red flags. These manual checks include GSA's Excluded Parties List System (EPLS), the Department of State Defense Trade Controls (DTC) list, and the US Department of Commerce Denied Persons List (DPL) among others. Beyond these initial checks, individuals are also screened to see if they are on other government owned derogatory-information lists – any of which could qualify an individual from TSC approval.

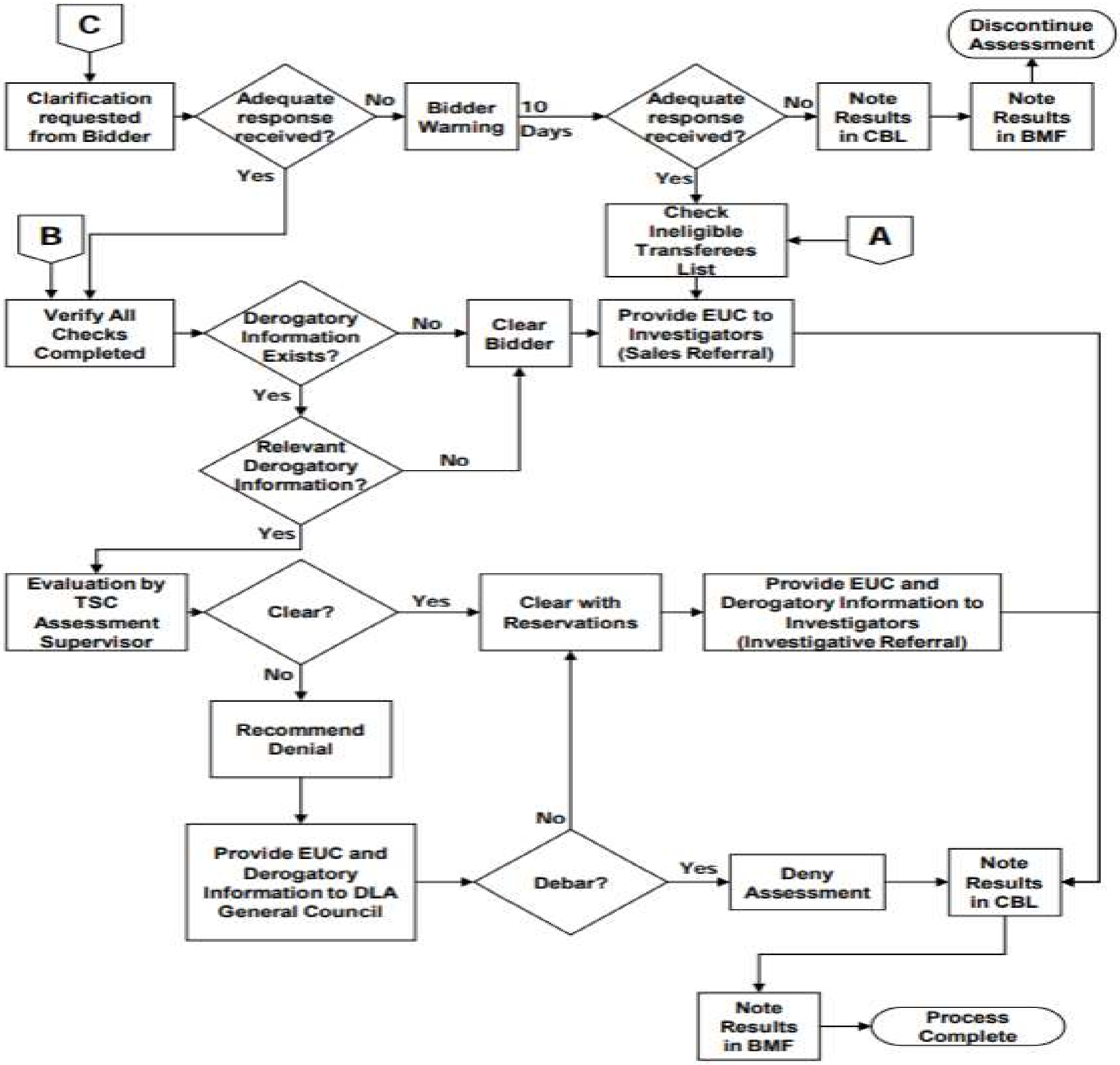
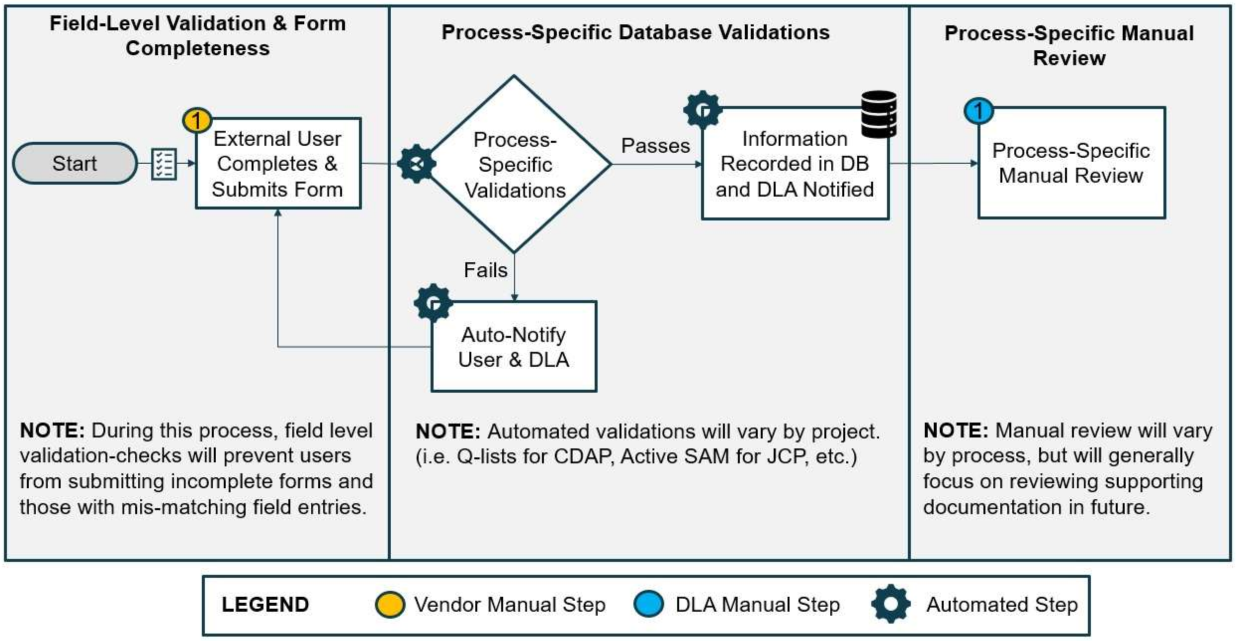

C
Clarification requested from Bidder
Adequate response received?
No
Bidder Warning
10 Days
Adequate response received?
No
Note Results in CBL
Note Results in BMF
Discontinue Assessment
Yes
Yes
Check Ineligible Transferees List
A
B
Verify All Checks Completed
Derogatory Information Exists?
No
Clear Bidder
Provide EUC to Investigators (Sales Referral)
Yes
Relevant Derogatory Information?
No
Yes
Evaluation by TSC Assessment Supervisor
Clear?
Yes
Clear with Reservations
Provide EUC and Derogatory Information to Investigators (Investigative Referral)
No
Recommend Denial
No
Provide EUC and Derogatory Information to DLA General Council
Debar?
Yes
Deny Assessment
Note Results in CBL
Note Results in BMF
Process Complete

Figure 35. *Part Two of Trade Security Control Process*

After passing the initial background and government agency checks, an individual can move through the TSC process only if they have no derogatory information found or if they are cleared with reservations by a qualified TSC representative. While this determination of 'qualified' versus 'not qualified' is key to the TSC process, most time within the TSC process is currently spent correcting user submissions and communicating with end users, as opposed to performing this core function. However, automation of key checks and the introduction of data validation checks should allow the process to streamline activities in the future and concentrate on core TSC tasks.

7.5 TSC Future State Processes

A major recommendation for all web-based data collection approaches is the inclusion of field-level validations prior to external user submission. These validations would serve two purposes: (1) preventing users from submitting incomplete forms and (2) preventing users from submitting data within a field that does not match the required data format (e.g. entering 'John Smith' in the Date field). By implementing these controls, DLA can ensure that TSC resources will only receive EUCs for review if they are compatible with these controls. These process controls have been recommended for CDAP in previous sections and are also recommended for the JCP process. The general flow of information from user submission, to automated checks, and finally into DLA databases for manual review is shown in Figure 36 below.


Field-Level Validation & Form Completeness
Process-Specific Database Validations
Process-Specific Manual Review
Start
1
External User Completes & Submits Form
Process-Specific Validations
Passes
Information Recorded in DB and DLA Notified
1
Process-Specific Manual Review
Fails
Auto-Notify User & DLA
LEGEND
Vendor Manual Step
DLA Manual Step
Automated Step

NOTE: During this process, field level validation-checks will prevent users from submitting incomplete forms and those with mis-matching field entries.

NOTE: Automated validations will vary by project. (i.e. Q-lists for CDAP, Active SAM for JCP, etc.)

NOTE: Manual review will vary by process, but will generally focus on reviewing supporting documentation in future.

Figure 36. *Future State Initial User Submission Process*

As shown above, a series of process-specific (will vary for CDAP, JCP, and TSC) automated checks will bolster field-level validation and completeness checks which should result in much higher-quality data being received by DLA resources. These 'initial checks' are represented in Figure 36 above and Figure 37 below as a page with checkmarks, indicating a form which has passed initial validations.

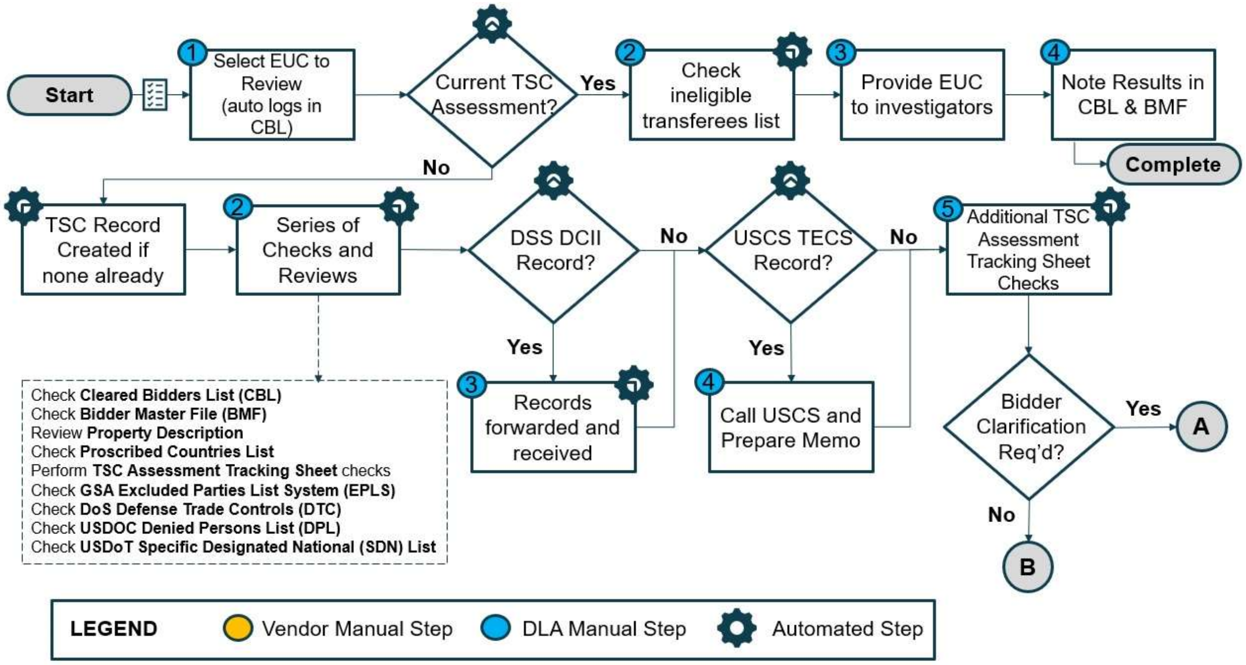

Start
1
Select EUC to Review (auto logs in CBL)
Current TSC Assessment?
Yes
2
Check ineligible transferees list
3
Provide EUC to investigators
4
Note Results in CBL & BMF
Complete
No
TSC Record Created if none already
2
Series of Checks and Reviews
DSS DCII Record?
No
USCS TECS Record?
No
5
Additional TSC Assessment Tracking Sheet Checks
Yes
Yes
3
Records forwarded and received
4
Call USCS and Prepare Memo
Check Cleared Bidders List (CBL)
Check Bidder Master File (BMF)
Review Property Description
Check Proscribed Countries List
Perform TSC Assessment Tracking Sheet checks
Check GSA Excluded Parties List System (EPLS)
Check DoS Defense Trade Controls (DTC)
Check USDOC Denied Persons List (DPL)
Check USDoT Specific Designated National (SDN) List
Bidder Clarification Req'd?
Yes
A
No
B
LEGEND
Vendor Manual Step
DLA Manual Step
Automated Step

Figure 37. *Part One of Trade Security Control Future State*

Other portions of the TSC process which are capable of introducing automation have been labeled with gear icons in the above process map. Since the TSC is a certification program required to reference a variety of online government sources, many of these checks can be automated via existing data interfaces or new internal table references. In particular, a large chunk of 'series and reviews' shown to the bottom left of the figure are recommended to be automated in a future state version of TSC.

In contrast to the relatively streamlined and automated plans for the initial phases of the TSC process, the latter portions of the process will remain largely unchanged or only slightly modified from the current state. This can be seen in Figure 38 on the following page, which contains most of the steps found in the original.

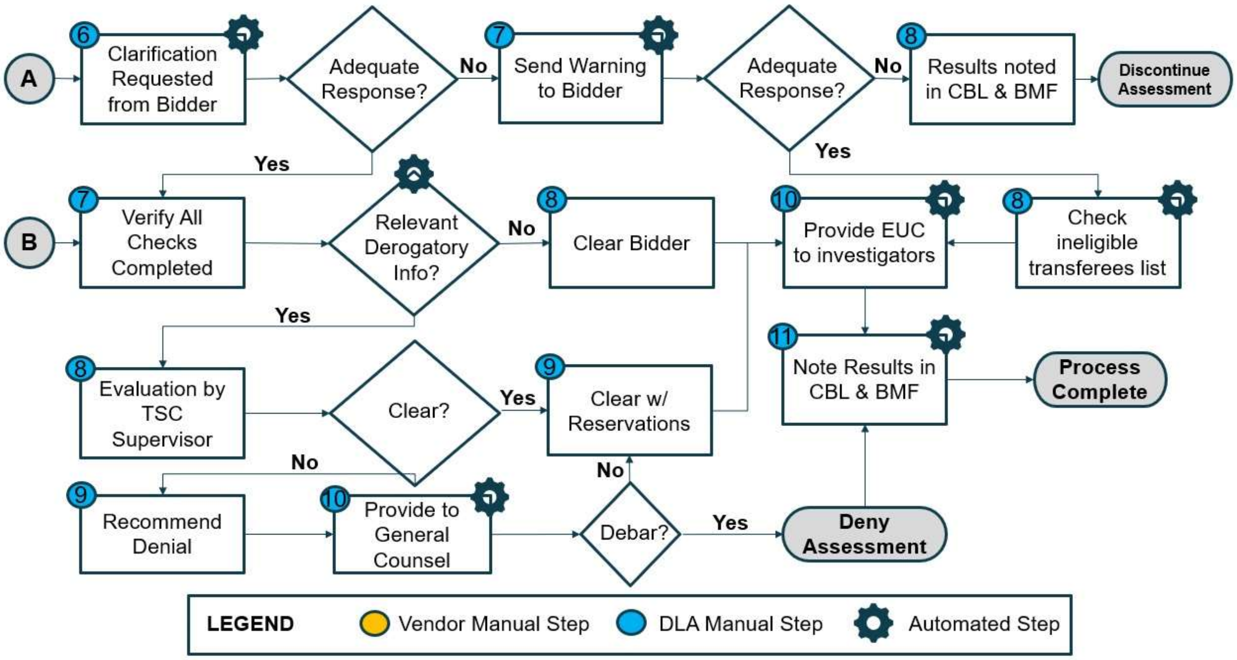


Figure 38. *Part Two of Trade Security Control Future State*

The largely manual and judgement-based nature of the latter TSC evaluation steps necessitate that most steps remain unchanged. As previously mentioned, these assessments – particularly when derogatory information is present – are critical to a properly functioning TSC process. By removing large portions of the previously manual up-front validation steps, this latter portion of the TSC process will become the core of the ‘human evaluation’ portion of the process and where most TSC resources will allocate the majority of review and/or collaboration time.

8.0 Joint Certification Program (JCP)

8.1 JCP Introduction

As part of the analysis of Trade Security Control processes, it was determined that the Joint Certification Program is a related complimentary effort with similar issues. This program is key to providing access to important export controlled technical data to certain DLA business partners and has also suffered severe backlog issues as a result of existing manually intensive processes. Additionally, the certification via DD Form 2345, of an individual's Nationality – among other pieces of information – also make the program a candidate for enhanced data collection with increased security measures. The following sections briefly describe the program, recommended future state processes, and ultimately recommended business requirements for collecting DD Form 2345 information via a web-based form.

8.2 JCP Background [2]

The Joint Certificate Program (JCP) was established to allow U.S. and Canadian contractors to apply for unclassified export controlled technical data. The DoD controls the export of unclassified technical data to preserve U.S. military data and technology. This data includes technical data or computer software that can be used in the design, production, manufacture, assembly, repair, overhaul, processing, engineering, development, operation, maintenance, adapting, testing, or reconstruction of goods or materiel; or any technology that advances the state of art, in an area of significant military or space applicability in the U.S. Availability of this data allows contractors to identify opportunities with the DoD and enables the scientific community to further research in technology.

The DoD proposed the *Withholding of Unclassified Technical Data and Technology From Public Disclosure* rule in 2016 to mitigate the risks associated with unclassified export controlled technical data. Access to this data by unauthorized users and foreign governments exposes the U.S. military technology, and endangers the military superiority of the U.S.

The JCP is managed by the Joint Certificate Office (JCO) who reviews and certifies the DD Form 2345 for thousands of contractors annually. A contractor granted an export-controlled certificate can participate in a variety of DoD activities such as program briefings and bidding on public contracts.

8.3 JCP DD Form 2345

As described above, DD Form 2345 is the primary documentation required for submitting a Joint Certification Program request. In addition to this form, external users are required to submit documentation verifying the legitimacy of their need to view unclassified export controlled technical data. This legitimacy documentation may include an Incorporation Certification, State

[2] **Source:** https://www.federalregister.gov/documents/2016/10/31/2016-26236/withholding-of-unclassified-technical-data-and-technology-from-public-disclosure

or Provincial Business License, or Sales Tax Identification Form. Basic information which is required as part of the standard DD Form 2345 submission are displayed in Table 14 below.

Table 14. *DD Form 2345 Data Element Types*

Data Element	Section	Data Type
Initial Submission	Type of Submission	Checkbox
Revision	Type of Submission	Checkbox
5-year Renewal	Type of Submission	Checkbox
Name	Enterprise or Individual Data	Character
Address	Enterprise or Individual Data	Free Text
Name of Subsidiary / Division / Department	Enterprise or Individual Data	Character
CAGE Code	Enterprise or Individual Data	Alphanumeric
Name	Data Custodian	Character
Telephone Number	Data Custodian	Numeric
Title	Data Custodian	Character
E-Mail Address	Data Custodian	Alphanumeric
Description of Relevant Business Activity	Relevant Business Activity	Free Text
The United States	Citizenship Certification	Checkbox
Canada	Citizenship Certification	Checkbox
Typed Name	Contractor Certification	Character
Title	Contractor Certification	Character
Signature	Contractor Certification	Digital Signature
Date Signed	Contractor Certification	Date
Certification Accepted	Certification Action	Checkbox
Number	Certification Action	Character
Expiration Date	Certification Action	Numeric
Typed Name	DOD Official	Character
Title	DOD Official	Character
Signature	DOD Official	Digital Signature
Date Signed	DOD Official	Date
Typed Name	Canadian Official	Character
Title	Canadian Official	Character
Signature	Canadian Official	Digital Signature
Date Signed	Canadian Official	Date

One unique aspect of the JCP process is that the user-submitted DD Form 2345 requires a series of ‘wet ink’ signatures to be considered valid. Recent discussions with the DLA Legal department have resulted in an initial agreement that legally binding digital signatures may be used to replace this ‘wet ink’ requirement in the future. This consideration is a key component of the modernization and digitization of the JCP process and is reflected in the functional and technical requirements for the program and digital web form.

8.4 JCP Current State Processes

The Joint Certification Program begins with the collection of a manually completed and mailed-in PDF form, just as the previously described CDAP and TSC processes are. Part of this requirement is due to the fact that a 'wet ink' signature is required from the individuals who are submitting documentation, to certify the legitimacy of their information. However, the requirement to submit paper copies of DD Form 2345 has exposed the program to a plethora of user-submission errors including incomplete forms and erroneous data. Information provided by JCP representatives has indicated that the initial rejection rates for the basic administrative correctness checks is between eighty to ninety percent, resulting in a substantial amount of time spent returning forms to users.

This process also includes the scanning of each form, so that a digital twin is created within DLA systems. The current state process maps for the JCP process are split into two main processes; (1) receiving and processing incoming mail and (2) reviewing and certifying the information. A general process map for the existing 'receiving and processing mail' steps are shown in Figure 39.

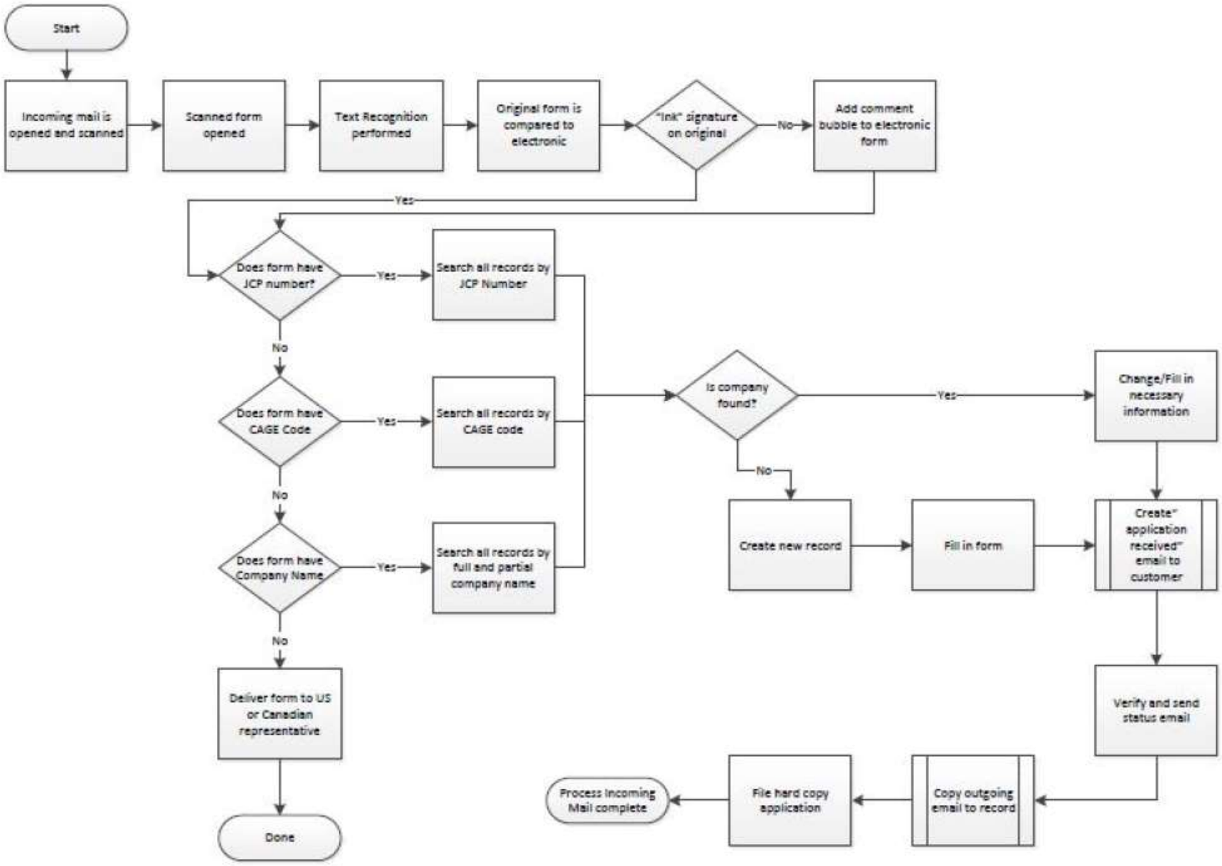

Start
Incoming mail is opened and scanned
Scanned form opened
Text Recognition performed
Original form is compared to electronic
"Ink" signature on original
No
Add comment bubble to electronic form
Yes
Does form have JCP number?
Yes
Search all records by JCP Number
No
Does form have CAGE Code
Yes
Search all records by CAGE code
No
Does form have Company Name
Yes
Search all records by full and partial company name
No
Deliver form to US or Canadian representative
Done
Is company found?
Yes
Change/Fill in necessary information
No
Create new record
Fill in form
Create" application received" email to customer
Verify and send status email
Copy outgoing email to record
File hard copy application
Process Incoming Mail complete

Figure 39. *JCP Current State Processes for Incoming Mail*

The steps required to receive and process incoming JCP records is time consuming, especially considering the high rate of errors and resubmissions required by external users. These factors have contributed, in part, to a current backlog in excess of 1,000 JCP records. Even in situations where external entities submit accurate and complete information, physical forms must be completely scanned in and attached to new or existing records after a series of checks.

The second part of the JCP process is the data review and validation. This portion of the process is key to determining an entities eligibility to access protected information and includes a multitude of DLA and government-based checks. The most important section of this process is the step labeled ‘check requirements’, where a variety of validations must occur. These are listed on the bottom left of Figure 40 below.

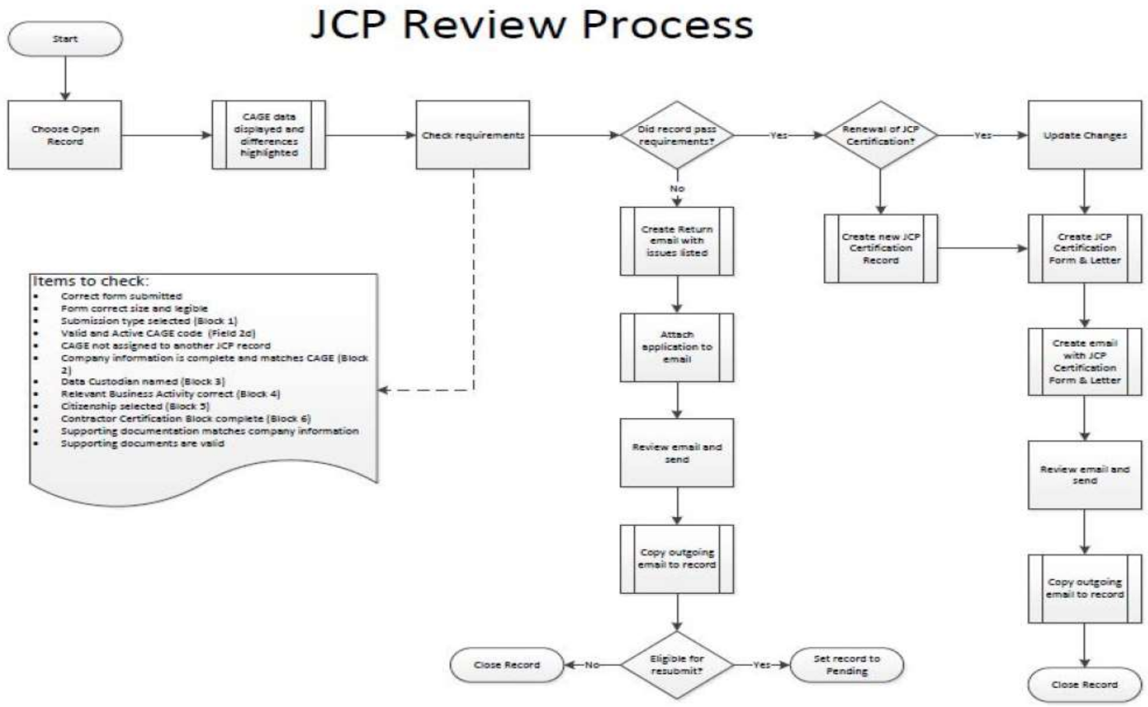

JCP Review Process
Start
Choose Open Record
CAGE data displayed and differences highlighted
Check requirements
Did record pass requirements?
Yes
Renewal of JCP Certification?
Yes
Update Changes
No
Create Return email with issues listed
Create new JCP Certification Record
Create JCP Certification Form & Letter
Items to check:
Correct form submitted
Form correct size and legible
Submission type selected (Block 1)
Valid and Active CAGE code (Field 2d)
CAGE not assigned to another JCP record
Company information is complete and matches CAGE (Block 2)
Data Custodian named (Block 3)
Relevant Business Activity correct (Block 4)
Citizenship selected (Block 5)
Contractor Certification Block complete (Block 6)
Supporting documentation matches company information
Supporting documents are valid
Attach application to email
Create email with JCP Certification Form & Letter
Review email and send
Review email and send
Copy outgoing email to record
Copy outgoing email to record
Close Record
No
Eligible for resubmit?
Yes
Set record to Pending
Close Record

Figure 40. *JCP Current State Review Process*

8.5 JCP Future State Processes

As previously noted, JCP resources have collaborated with DLA Legal to determine that end user signatures on future JCP (and potentially other) forms can be replaced with appropriate 'digital signature' approaches. A digital signature is a cryptographically generated digital representation of a person's physical (or 'wet ink') signature and a valid legal replacement, given appropriate generation guidelines. With this approval in place, the possibility for JCP forms to be submitted digitally and processed as shown previously in Figure 36 will be possible. This will not only remove the likelihood of incomplete forms being submitted, but also reduce the likelihood of a field-level error and remove the requirement for forms to be digitally scanned once received by DLA.

With the addition of three automated validations intended to determine whether the submitter has an active System for Awards Management (SAM), CAGE, and/or Data Universal Numbering System (DUNS) the electronic data receipt process is greatly simplified for JCP. This improved process is shown in Figure 41.

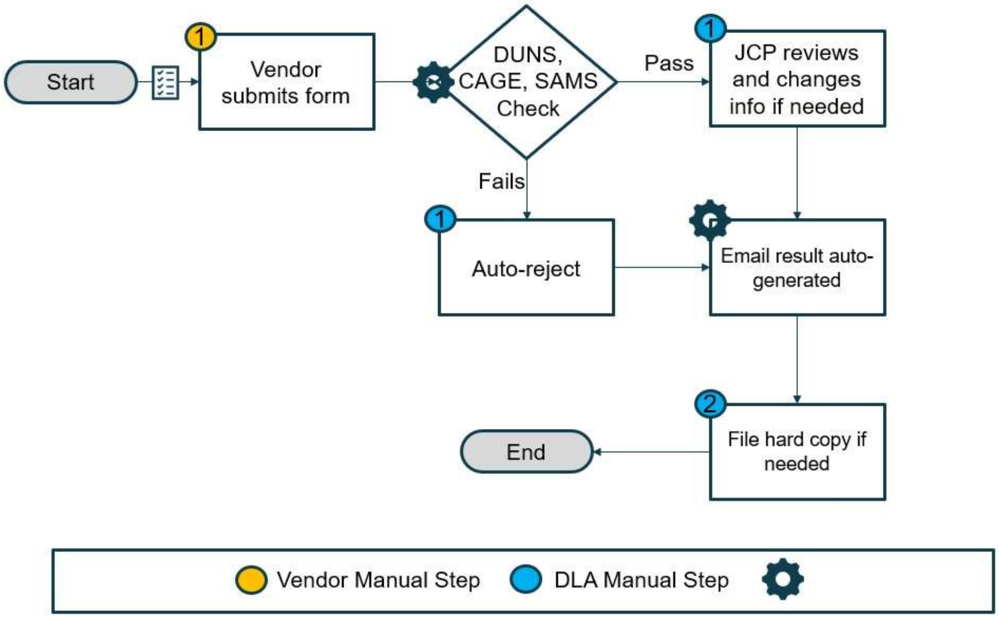


Figure 41. *Future State JCP Receipt Process*

By receiving the forms electronically, most (if not eventually all) of the JCP receipt process can be automated. The latter JCP Review process requires more manual attention and collaboration as shown in Figure 42 on the next page.

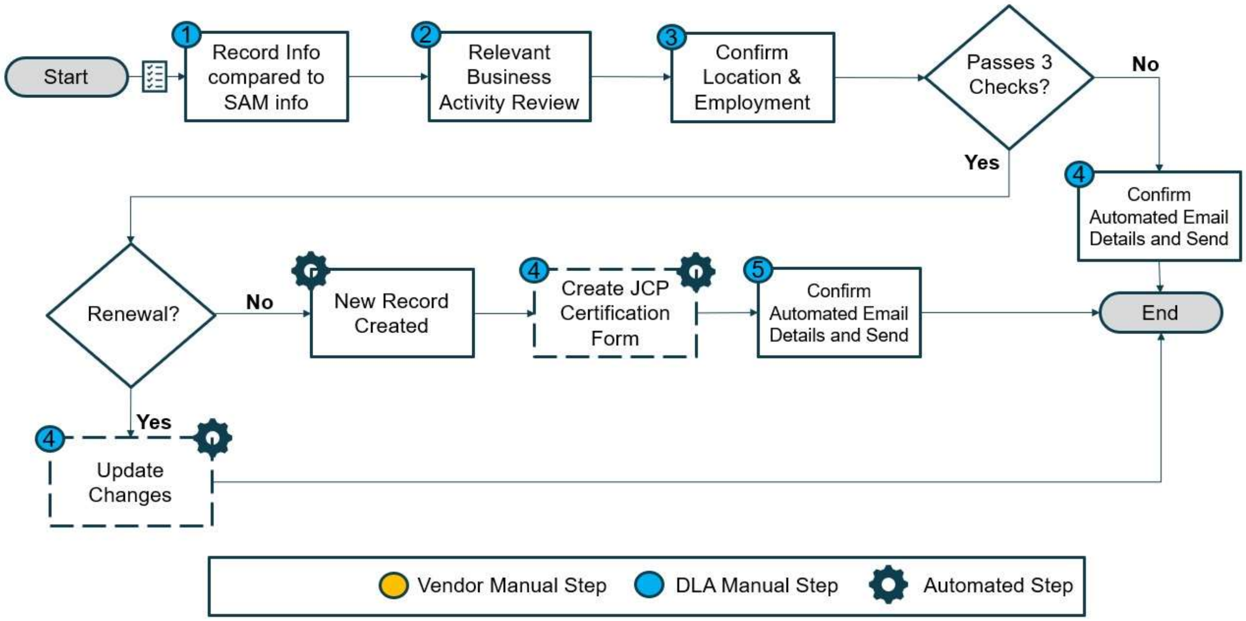

Start
1
Record Info compared to SAM info
2
Relevant Business Activity Review
3
Confirm Location & Employment
Passes 3 Checks?
No
Yes
4
Confirm Automated Email Details and Send
Renewal?
No
New Record Created
4
Create JCP Certification Form
5
Confirm Automated Email Details and Send
End
Yes
4
Update Changes
Vendor Manual Step
DLA Manual Step
Automated Step

Figure 42. *Future State JCP Review Process*

Along with the various database checks and reviews that may be automated in the future, there exist certain synergies that can be gained between the TSC, JCP, CDAP, and other Technical Quality programs. These programs often include some form of 'risk assessment' and the various internal DLA and external government-partner 'checks' typically help program employees make determinations on external users' fitness to be certified. For example, certain individuals submitting DD Form 1822 for Trade Security Control access can attest on that form that they are submitting their request in connection with a Joint Certification Program DD Form 2345.

Recent developments within DLA have enabled better data management and aggregation of vendor data, including information which can indicate a presence, or lack thereof, risk factors. The enterprise Business Decision Analytics (BDA) capability, for example, can provide ad hoc supplier reports with information pertaining to a CAGE-or-DUNS registered company's financial, legal, and compliance risk. BDA can also identify key DLA qualifications such as 'QTSL' and displays this information juxtaposed with DoD-wide Supplier Performance Retrieval System (SPRS) information.

As DLA digitizes the collection of these forms, new qualifications will be stored within DLA systems and new ways of streamlining and automating these processes will become possible. The following section lists detailed recommended business process requirements for all three previously discussed programs – (1) Counterfeit Detection and Avoidance Program, (2) Trade Security Control, and (3) Joint Certification Program. These recommended requirements can form the basis for a J6 Front Door submission, which is the next step toward modernizing these processes.

9.0 Recommended Business Requirements

The Digital Traceability implementation aims to develop a method for hosting digital web-based forms for collecting external user data to facilitate processes required for the Counterfeit Detection and Avoidance Program (CDAP), Trade Security Control (TSC), and the Joint Certification Program (JCP). The following assumptions and general recommended business requirements apply broadly to all three of these stakeholder groups/processes. However, there are some requirements specific to each group, which are listed below their applicable headers. Additionally, more detailed requirements for a CDAP visualization are listed at the end, while no specific visualization requirements are included for either TSC/JCP. There is, however, an assumption that DLA leadership will determine whether to build business intelligence visualizations for the TSC and JCP programs.

9.1 Assumptions

1. Requirements provided by the application and process Subject Matter Experts (SMEs) are the basis of these requirements.
2. Business requirements will be re-confirmed with application SMEs during integration with the EBS program.
3. The scope of this application analysis is to determine how the existing processes and system functions may be modernized on a Digital Platform with processes re-engineered as appropriate.
4. A Digital Platform such as Salesforce or Microsoft PowerApps is already deployed at DLA and in EBS.
5. An Enterprise Identity Management (IDM) solution is available with which the Digital Platform can integrate and offers user self-registration capability.
6. Availability and support from all involved teams will be required; e.g. Application Security (J6K), Chief Data Officer (CDO) office, and other EBS technical delivery teams.
7. Digital Traceability will operate under EBS ATO (Authority to Operate) designation.
8. DLA stakeholders will determine whether collected data and attached documentation should be stored or utilized within the Enterprise Business Systems (EBS) and/or Enterprise Data Warehouse (EDW) among storage options.
9. DLA will allocate enough storage space and/or data tables to house information collected for the CDAP, TSC, an JCP programs including but not limited to collected Form data and attached documents.
10. DLA stakeholders leading each process area (CDAP, TSC, and JCP) will decide whether business intelligence dashboards and/or metrics will be developed as part of the Digital Traceability effort or separately with J6 via enterprise visualization efforts.
11. DLA J6 will provide CDAP, TSC, and JCP end users with software access and the hardware required to view visualizations built for them using the DLA Enterprise Visualization tool (if applicable).

12. DLA J6 will provide final guidance on whether software extensions may be utilized in the development of the business intelligence dashboards.

13. If identity management is required by DLA as part of the user submission of data via a web-based form, J6 will provide applicable requirements for that process.

14. In conjunction with DLA J6, process area leadership for CDAP, JCP, and TSC will determine whether an external user-registration process will be needed to digitally sign documents and review submission statuses.

9.2 Recommended Business Requirements

9.2.1 Recommended General Requirements

1. The Digital Traceability implementation shall include the development web-based forms for collecting information and supplemental documentation, in the form of file attachments, from external vendors.

2. All web-based forms shall be accompanied by data dictionaries to define data elements required for each process area.

3. Components of the Digital Traceability implementation will be accessible to each stakeholder group as outlined in a future Segregation of Duties (SoD) document developed by DLA.

4. If cloud hosting is required, the system shall be hosted on an Impact Level (IL) 4/5 Federal Risk and Authorization Management Program (FEDRAMP)-certified cloud environment (e.g. Azure US Gov. Virginia region).

5. The system shall be Risk Management Framework (RMF) accredited with Authority to Operate (ATO) from assigned Application ISSM.

6. The system shall accept DLA Common Access Cards (CAC) for DLA users.

7. The system shall control access based on specific user profiles (e.g. external end user, backend DLA user, system administrator, etc.).

8. The system shall allow all end users (both internal and external) to perform primary functions such as the ability to access web forms, submit web forms, and view submission statuses.

9. The system shall allow internal DLA users to add new records and update existing records based on their user profile.

10. The system shall allow internal DLA users to add free-form text and/or comments to each record.

11. The system shall allow internal DLA users to import data from Microsoft Excel.

12. The system shall allow internal DLA users to export data.

13. The system shall encrypt and securely transmit all submitted data as required by data handling compliance procedures.

14. The system shall store all data in a secured manner.

15. The system shall provide notification capabilities to notify assigned parties of any status changes in the system.

16. The system shall provide assignment capabilities which will allow submission records to be assigned to specific resources for review.

17. The system shall provide the capability to produce auditable artifacts when necessary.

9.2.2 Recommended General Digital Form Requirements

18. The Digital Traceability web-based forms will be Section 508 accessibility compliant.

19. The Digital Traceability web-based forms will be designed in collaboration with specific process-area stakeholders and technical support staff to have consistent and intuitive user interfaces (UI) with appropriate validation and instructions to help improve ease of use and reduce error rates.

20. The Digital Traceability web-based forms will be hosted online as a subset of DLA.mil or another existing DLA webpage.

21. The Digital Traceability web-based forms will be built and hosted with FEDRAMP compliant software.

22. The Digital Traceability web-based forms will be accessible to both internal and external users, with different access rights.

23. The Digital Traceability implementation will require at least one interface per digital form to collect information submitted through the web-based forms.

24. Data and documentation submitted through the web-based forms should be stored and accessible from process leads chosen data storage location within EBS or the EDW.

25. The Digital Traceability web-based forms will be compatible with major standard web browsers such as Internet Explorer, Chrome, and Firefox.

26. The Digital Traceability web-based forms will be accessible to external users without the use of a common access card (CAC).

27. The Digital Traceability web-based forms will provide help text or a means for information about the fields to be conveyed to users.

28. The Digital Traceability web-based forms may provide external users with capabilities to review and manage their submissions and submission statuses.

29. The Digital Traceability web-based forms will provide a summarized overview of all submitted information for user confirmation before being sent to DLA systems.

30. The Digital Traceability web-based forms will require external users to digitally sign or otherwise authenticate the form before confirming their information and submitting it.

31. The Digital Traceability web-based forms will provide a method for submitting the information and attachments (i.e. a submit button).

32. The Digital Traceability web-based forms will indicate submittal success or failure to users after they submit the information.

33. The Digital Traceability web-based forms will automatically produce an internal timestamp when information is submitted by an external user.

34. The Digital Traceability web-based forms will include built-in validation rules to ensure proper data formats for certain fields prior to submission and according to field characteristics in the data dictionary, as applicable.

35. The system shall check all fields before data transmission to prevent all web-based attacks.

36. The Digital Traceability web-based forms shall provide digital signature capabilities for capturing legally binding user signatures.

37. The system shall provide reporting capabilities on submitted data including statuses of requests (i.e. In Progress, Returned, Rejected, etc.)

9.2.3 Recommended CDAP Digital Form-918 Requirements

38. The CDAP web-based form will provide a method for submitting Traceability Documentation files.

39. The CDAP web-based form will provide a method for submitting additional Traceability Documentation files beyond the first.

40. The CDAP web-based form will provide a method for collecting, at a minimum, all information that is currently collected via Form 918.

41. The CDAP web-based form will be accessible from the main DLA website where DLA Land & Maritime CDAP information currently resides.

42. The DT web-based form will include a Supplier Information section requiring the following information about the external vendor:

a. Supplier Name

b. Supplier Address

i. Street

ii. City

iii. State

iv. Country

v. ZIP code

c. Commercial and Government Entity (CAGE) code

d. Point of Contact / Submitter Name

e. Point of Contact / Submitter Email

f. Point of Contact / Submitter Phone Number

43. The CDAP web-based form will include a Submitter Information section requiring the following information about the person submitting the form:

a. First Name

b. Last Name

c. Email

d. Phone Number

44. The CDAP web-based form will include a Contract Information section requiring the following information about the contract:

a. Contract Number

b. Contract Line Item umber (CLIN)

45. The CDAP web-based form will include an Item Information section requiring the following information about the item:

a. Item Name

b. Federal Supply Classification (FSC) code

c. National Item Identification Number (NIIN)

d. Part Number

e. Original Part Manufacturer

f. Manufacturer CAGE Code

46. The CDAP web-based form will provide a method (radio button, check box, etc.) for indicating whether an external vendor has changed their Name, Address, or Logo.

a. If the external vendor indicates 'YES', they have changed their Name, Address, or Logo the DT web-based form will provide a free text box for external vendors to describe their modified information and the ability to upload supporting documentation files.

b. If the external vendor indicates 'YES', they have changed their Name, Address, or Logo the DT web-based form will provide a method for submitting supporting documentation files.

47. The CDAP web-based form will include a Quantity / Date Code section requiring the following information about the items:

   a. Date Code

   b. Quantity

   c. Country of Origin

48. The CDAP web-based form will provide a method for entering multiple unique Date Code and Quantity combinations.

49. The CDAP web-based form will provide a Traceability Documentation Type including a method for the external vendor to certify their level of qualification with the following options:

   a. Approved Source Manufacturer Specified in the Solicitation/Contract Item Description (Original Component Manufacturer (OCM), Original Equipment Manufacturer (OEM),

   b. Approved Source on the Applicable Qualified Products List (QPL) / Qualified Manufacturers List (QML),

   c. Authorized Distributor of the OCM/OEM or QPL/QML Approved Source,

   d. Supplier Distributor on the Qualified Suppliers List of Distributors (QSLD),

   e. Supplier/Distributor on the Qualified Testing Suppliers List (QTSL) for FSC 5961/5962

50. The CDAP web-based form will provide a method for viewing information / help text about each of the qualification levels (i.e. QSLD, QSLM, QML, etc.) and what types of Traceability Documentation are required for each.

51. The CDAP web-based form will include a Type of Documentation section including a method for the user to select the type of Traceability Documentation they are submitting from the following choices:

   a. Traceability Document(s)

   b. Test Report(s)

52. The Digital Traceability solution will generate a Post Award Request assigned to CDAP users when information has been successfully submitted via the CDAP web form.

9.2.4 Recommended TSC Digital DD Form 1822 Requirements

53. The TSC web-based form will provide a method for collecting, at a minimum, all information that is currently collected via DD Form 1822.

54. The TSC web-based form will provide detailed user instructions for each field/block on DD Form 1822.

55. The TSC web-based form will allow users to attach/upload supplementary documentation.

56. The TSC implementation will include a method for tracking process metrics.

57. The TSC implementation will automatically record and store user submitted data to an Enterprise TSC data storage location.

58. The TSC implementation will automatically record and store TSC-related metrics within an Enterprise TSC data storage location on a recurring basis.

59. The TSC implementation will include metrics to measure the following record statuses:

a. In-process Record Reviews

b. Returned Records (Including Subsets for Various 'Return Reasons')

c. Resubmitted Records

d. Rejected Records

e. Certified Records

f. Debarred Records

60. The TSC implementation will include a method for automatically producing periodic reports (i.e. daily, weekly, monthly production reports).

61. The TSC implementation will include a method for executing reports on an ad hoc basis.

62. The TSC implementation will include internal workload management capabilities.

63. The TSC implementation will include a method for automatically alerting resources when new records have been submitted that pass validation checks or are rejected.

64. The TSC implementation will have the capability to send automate notices to external email addresses (external users) to notify them of upcoming certification expiration.

65. Internal TSC functionality will include record search capabilities.

66. Internal TSC functionality will include the ability to add new records and edit existing records.

67. Internal TSC functionality will include a means for adding free-form text/comments to each record.

68. Internal TSC functionality will include a capability for importing data within MS Excel workbooks.

69. Internal TSC functionality will include a capability for exporting data records.

70. The TSC web-based form will include a header section allowing the submitter to indicate whether the statement is submitted in connection with any of the following (checkboxes):

a. Sale

b. Exchange

c. DD2345

d. Other (allow free form text)

71. The TSC web-based form will include a section for the user to enter the following information in free-form text:

  a. Line Item Number/Commodity/Technical Data Request
  b. Name
  c. SSN/Alien Card No./Country ID
  d. Date of Birth
  e. Place of Birth
  f. Telephone Number
  g. Mailing Address
  h. Physical Address

72. The TSC web-based form will include a Section I General Information with spaces to enter the following information:

  a. Type of Firm (checkboxes)
    i. Sole Proprietorship
    ii. Partnership
    iii. Corporation
    iv. Corporation with Sole Officer
    v. Other (allow freeform text)
  b. Nature of End-User's Business
  c. Nature of Principal's Business
  d. Firm's ID/Federal Tax Number
  e. Business/Corporation Headquarters
    i. Name
    ii. Address
  f. Branch Office
    i. Name
    ii. Address

73. The TSC web-based form will include a free-text box at the top of Section II End Use/User Information with instructions "If this is a negotiated exchange, identify the property being exchanged."

74. The TSC web-based form will include Section II End Use/User Information where the user can check any of the following to indicate the 'Purpose' of the request:

a. Retention for the following specific use (allow free form text)

b. Resold or retransferred in the form received for the following use (allow free form text)

c. The property will not be sold or otherwise transferred or disposed of for use outside of the United States or to non-U.S. Citizens/Nationals in the United States.

d. The property may be exported or re-exported in the form received to the following country/countries. (allow free form text)

e. Resale after following alteration (description of final production) – (allow free form text) - in (Country/Countries) (allow free form text) - and distribution in (country/countries) - (allow free form text).

f. If sold or retransferred, name, address, and telephone number of sub-purchaser(s)/sub-contractor(s) (allow free form text).

g. The customers are unknown at this time. If required by the contract/transfer document, I will obtain prior written approval for the resale of any of the property covered by this contract.

75. The TSC web-based form will include a large free form text box for entry of Additional Information.

9.2.5 Recommended JCP Digital DD Form 2345 Requirements

76. The JCP web-based form will provide a method for collecting, at a minimum, all information that is currently collected via DD Form 2345.

77. The JCP web-based form will provide detailed user instructions for each field/block on DD Form 2345.

78. The JCP web-based form will allow users to attach/upload supplementary documentation.

79. The JCP implementation will include a method for tracking process metrics.

80. The JCP implementation will automatically record and store user submitted data to an Enterprise JCP data storage location.

81. The JCP implementation will automatically record and store JCP-related metrics within an Enterprise JCP data storage location on a recurring basis.

82. The JCP implementation will include metrics to measure the following record statuses:

a. In-process Record Reviews

b. Returned Records (Including Subsets for Various ‘Return Reasons’)

c. Resubmitted Records

d. Rejected Records

   e. Certified Records

   f. Debarred Records

83. The JCP implementation will include a method for automatically producing periodic reports (i.e. daily, weekly, monthly production reports).

84. The JCP implementation will include a method for executing reports on an ad hoc basis.

85. The JCP implementation will include internal workload management capabilities.

86. The JCP implementation will include a method for automatically alerting resources when new records have been submitted that pass validation checks or are rejected.

87. The JCP implementation will have the capability to send automate notices to external email addresses (external users) to notify them of upcoming certification expiration.

88. Internal JCP functionality will include record search capabilities.

89. Internal JCP functionality will include the ability to add new records and edit existing records.

90. Internal JCP functionality will include a means for adding free-form text/comments to each record.

91. Internal JCP functionality will include a capability for importing data within MS Excel workbooks.

92. Internal JCP functionality will include a capability for exporting data records.

93. The JCP web-based form will include a section for the user to indicate the Type of Submission (checkboxes) from the following choices:

   a. Initial Submission

   b. Revision

   c. 5-year Renewal

94. The JCP web-based form will include an Enterprise of Individual Data section with spaces to enter the following (allow free form text):

   a. Name

   b. Address

   c. Name of Subsidiary/Division/Department

   d. CAGE Code

95. The JCP web-based form will include a Data Custodian section with spaces to enter the following (allow free form text):

   a. Name

   b. Telephone Number

   c. Title

d. E-Mail Address

96. The JCP web-based form will include a Description of Relevant Business Activity section with a large free form text box to allow users to enter an explanation.

97. The JCP web-based form will include a section for the user to certify whether they are a U.S. or Canadian Citizen (checkboxes):

a. United States Citizen

b. Canadian Citizen

98. The JCP web-based form will include a section for the user to enter the following Contractor Certification information (allow free form text):

a. Typed Name

b. Title

c. Signature

d. Date Signed

9.2.6 Recommended CDAP Visualization Functionality Requirements

99. The CDAP dashboard will have a main landing page called CDAP Workload Overview including key metrics showing the number of solicitations and awards in various stages of the procurement/CDAP processes including:

a. Open Solicitations

b. Awards Awaiting Documentation

c. Traceability Needing Review

d. Awards at DDWO

e. Awards at Test Lab

f. CDAP Completed Awards

100. The CDAP Workload Overview page will include average time metrics below each of the stages of procurement/CDAP including:

a. Average Time to Award

b. Average Time to Receive Documentation

c. Average Time to Review

d. Average Time to Ship

e. Average Time for Quick Look

f. Average Time in Test Lab

101. The CDAP Workload Overview page will include a Supplier Classification donut chart depicting the Supplier Classification of external vendors who have traceability reviews in process including the following categories:

a. OEM

b. OCM

c. QPL

d. QTSL

e. QML

f. QSLD

102. The CDAP Workload Overview page will include a Closed Awards donut chart depicting the status of closed awards from a chosen period of time including:

a. Award Completed

b. Award Cancelled

103. The CDAP Workload Overview page will include an Award Status donut chart depicting the status of awards including:

a. Open Solicitation

b. Awards Awaiting Documentation

c. Traceability Needing Review

d. Awards at DDWO

e. Awards at Test Lab

f. CDAP Completed Awards

104. The CDAP dashboard will have a screen for analyzing information about Open Solicitations including the following fields:

a. Open Solicitations (Count)

b. Closed Awards (Count)

c. Cancelled Awards (Count)

105. The Open Solicitations page will include a pie chart comparing the following metrics:

a. Open Solicitations Pending Award (Count)

b. Closed Solicitations Awarded (Count)

c. Closed Solicitations Cancelled (Count)

106. The Open Solicitations page will include an Awards Pending (Days Since Closed) histogram depicting a distribution of closed solicitations and the number of days they have been closed without an award made.

107. The Open Solicitations page will include a table of the CDAP catalog, filtered to show only entries that are Open Solicitations.

108. The CDAP dashboard will have a screen for analyzing information about Awards Awaiting Documentation including the following fields:

a. Delinquent Traceability Documentation (Count)

109. The Awards Awaiting Documentation page will include a Traceability Pending Time donut chart depicting the percentage of awards that are:

a. Awaiting Documentation (< 15 days)

b. Late Documentation (approximately 15 days)

c. Overdue Documentation (approximately 20 days)

110. The Awards Awaiting Documentation page will include a Historical Delinquency of Awards by Month stacked bar graph comparing the historical delinquency of awards by month, separated by the award's documentation status:

a. Awaiting Documentation (< 15 days)

b. Documentation Late (approximately 15 days)

c. Documentation Overdue (approximately 20 days)

111. The Awards Awaiting Documentation page will include a table of the CDAP catalog, filtered to show only entries that are Awards Awaiting Documentation.

112. The CDAP dashboard will have a screen for analyzing information about awards with Traceability Needing Review including the following fields:

a. Traceability Documentation Needing Review (Count)

b. Average Number of Resubmissions (Per Award)

113. The Traceability Needing Review page will include an Outstanding Traceability Review histogram showing the count of awards needing traceability review by number of days since traceability documentation was received by CDAP.

114. The Traceability Needing Review page will include a Supplier Classification pie graph showing the number of traceability documents submitted by each supplier type:

a. OEM

b. OCM

c. QPL

d. QTSL

e. QML

f. QSLD

115. The Traceability Needing Review page will include a Traceability Type donut chart comparing the type of traceability documentation:

a. Test Report

b. Traceability Documentation.

116. The Traceability Needing Review page will include a Type of Error donut chart depicting the breakdown of the type of error submitted:

a. Contract Information

b. Documentation

c. Documentation Type

d. Item Information

e. Qty/Date Codes

f. Supplier Information

g. Submitter Information

117. The Traceability Needing Review page will include an Average Time to Complete Traceability bar graph depicting the average time to complete traceability reviews from each month.

118. The Traceability Needing Review page will include a table of the CDAP catalog, filtered to show only entries that are Traceability Needing Review.

119. The CDAP dashboard will have a screen for analyzing information about Awards at the DDWO.

120. The Awards at DDWO page will include a Quick Look Fail Rate by Month stacked bar graph comparing the following fields across all 12 months:

a. Failed Quick Look inspection (Count)

b. Passed Quick Look inspection (Count)

121. The Awards at DDWO page will include a Quick Look Fail Rate by Supplier Type stacked bar graph comparing the following fields for OCM, OEM, QML, QPL, QSLD, and QTSL supplier types:

a. Failed Quick Look inspection (Count)

b. Passed Quick Look inspection (Count)

122. The Awards at DDWO page will include a table of the CDAP catalog, filtered to show only entries that are Awards at DDWO.

123. The CDAP dashboard will have a screen for analyzing information about Awards at the Test Lab.

124. The Awards at Test Lab page will include a Test Lab Fail Rate by month stacked bar graph comparing the following fields across all 12 months:

a. Failed Test Lab testing (Count)

b. Passed Test Lab testing (Count)

125. The Awards at Test Lab page will include a Test Lab Fail Rate by Supplier Type stacked bar graph comparing the following fields for OCM, OEM, QML, QPL, QSLD, and QTSL supplier types:

a. Failed Test Lab testing (Count)

b. Passed Test Lab testing (Count)

126. The Awards at Test Lab page will include a table visualization of the CDAP catalogue, filtered to show only entries that are Awards at Test Lab.

127. The CDAP dashboard will have a screen for analyzing information about CDAP Completed Awards.

128. The Closed Awards page will include Closed Award Distribution by Month stacked bar graph comparing the following fields across all 12 months:

a. Awards Cancelled (Count)

b. Awards Completed (Count)

129. The Closed Awards page will include a Closed Award Reasons pie chart distribution comparing the following closed award type fields:

a. Alternate Materiel Not Acceptable

b. Contract Compliance

c. Discovered Fraud

d. Quick-Look Failed

e. Traceability Documentation Failed

f. User-Error

130. The Closed Awards page will include a table visualization of the CDAP catalog, filtered to show only entries that are Awards at Closed Awards.

10.0 Proposed Technical Considerations

The goal of this research and development program is to recommend technical recommendations and considerations for modernization of these three programs via recommended business requirements and technical considerations. The intent of this section is to convey relevant technical specifications to DLA J6 Information Operations for appropriate design of a future state enhancement.

10.1 Application Modernization Recommendation

Proposed technical approach is to re-engineer existing processes and migrate existing Information Technology (IT) functionality and data stores into EBS on a fit-for-purpose Digital Platform (Platform-as-a-Service (PaaS)) Model which presents many benefits over utilizing existing systems such as:

- Limit ERP customization with an integrated solution that includes Analytics and AI capabilities.
- Reduced Total Cost of Ownership (TCO) with elimination of costs associated with hardware, infrastructure and upgrade efforts.
- Greater flexibility with re-usable APIs and microservices architecture.
- Low-Code No-Code capability empowers "Citizen Developer".
- Faster prototyping and delivery.
- Improved User Experience (UX) and efficiency.
- Reduced trouble tickets with input data validation.
- Cloud-first and as-a-Service model.
- Insights into Key Performance Indicators (KPI) with built-in self-service reporting capability.
- Eliminate environment contention on existing infrastructure with other EBS in-flight and future EBS projects and the need for DISA support.

10.2 Application Considerations

10.2.1 Project Management Considerations

- **Agile Methodology**
  - Agile methodology is the prevalent delivery framework in EBS which promotes increased collaboration between all stakeholders throughout the duration of the project, resulting in faster delivery time and consistent expectation of deliverable artifacts and scope of services

- **Efficient IT with DevSecOps**
  - DevSecOps ecosystem of tools will be leveraged to build, secure, test and deploy in a consistent and automated fashion to ensure efficient IT operations for CDAP/JCP/TSC applications

- **Testing Approach**
    - Project will leverage existing EBS testing methodology, which focuses on early mitigation of risks and issues. All testing cycles will be executed as necessary (with as much automation as possible):
        - System Integration
        - Security Role
        - Interoperability
        - Section 508
        - User Acceptance Testing (UAT)
        - Regression

Project team will deliver a Monthly Progress Report (MPR) to senior DLA J62L leadership on program activities including deliverable progress, project plan, accomplishments and future plans.

10.2.2 External Data Integration Considerations

If the DoD 5015.2 standard is necessary for Digital Traceability program, SAP Records Management (RM) will need to be utilized to store user submitted records such as PDF, image documents and invoice in order for artifacts to be stored and tracked in the same fashion as other EBS processes today. Transmitting data from Digital Platform to SAP RM (a component within EBS ECC system) will require a new integration point between the 2 systems as well as data transformation methods in order for artifacts to be stored. No other external partner connectivity identified from existing processes.

10.2.3 EDW Integration Considerations

Depending on the storage requirements and platform considerations, EDW's existing Data Lake can be used to store raw data in a more cost-friendly way. Custom integration point between the 2 systems will be needed.

10.2.4 User Base Considerations

- **System Administration / Developer**
    - Less than 20 for CDAP/JCP/TSC

- **End Users**
    - 30+ DLA users
    - 1,000+ DoD non-DLA users (majority don't use the system more than once a month)
    - Application allows external users (vendors) to submit data

10.2.5 Data Considerations

EDW Data Lake

- User data can be stored or its extracts submitted to EDW Big Data's Data Lake for advanced analytics and reporting

Volume

- CDAP Database currently maintains 20,000 entries (as of 05/31/2019), with a total database size of 200 GB.
- JCP Database currently maintains 25,000 entries (as of 05/31/2019), with a total database size of 200 GB
- TSC Database currently maintains 25,000 entries (as of 05/31/2019), with a total database size of 200 GB

Retention

- CDAP/JCP/TSC programs have the following data retention periods: Retain data for 10 years for CDAP; 15 years for JCP and TSC.
- CDAP/JCP/TSC programs do not actively archive or delete any records at this time.

10.2.6 Information Assurance / Security Considerations

- **Mission Assurance Category Level**
    - If migrated to under EBS technical accreditation boundary, a Mission Assurance Category (MAC) level of three would be applied to reflect EBS's standard including compliance with the DoD Risk Management Framework (RMF) in collaboration with J62LC Compliance team, the Information System Security Manager (ISSM) and Information System Security Office (ISSO) in order to obtain Authority to Operate (ATO)

- **Data backup, restore, or COOP requirements**
    - Existing data backup, restore, and COOP requirements would still apply

- **Data encryption requirements**
    - Existing and desired future data encryption requirements would still apply

- **Application and data access with associated role mappings**
    - If migrated to under EBS technical accreditation boundary, new AMPS and EBS roles would need to be created or existing AMPS and EBS roles would need to be updated to provide access to CDAP/JCP/TSC functionality

- **Segregation of Duties Analysis**
    - Existing Segregation of Duties policies as defined by current CDAP/JCP/TSC functionality would still apply and implemented based on RBAC (Role-based Access Control)

- **Other Security Considerations being implemented, monitored and reported by various teams on existing EBS applications and environments:**
    - Automated Device Discovery and Management
    - Automated Software Discovery and Management
    - Continuous Device and Network Monitoring
    - Automated Alerting/Reporting
    - Vulnerability Management

- Patch Management
- Configuration/Compliance Management
- Event Management
- Incident Management
- Cyber Policy Enforcement
- Automated Tool Orchestration
- Automated Network Access Control
- Data Rights Management and Data Loss Prevention
- Identity, Credential and Access Management

10.2.7 Technical Considerations

- **Service-Level Agreement (SLA)**
  - Availability and Performance SLAs are provided by the service provider (e.g. DISA, Cloud Service Provider such as Microsoft Azure or Platform-as-a-Service host provider)
  - Helpdesk Ticket and Defect Resolution SLAs follow EBS' standards

- **Emergency/Maintenance Window Support**
  - EBS' schedule and Standard Operating Procedure (SOP) will be adhered including participation in Technical Control Board (TCB) calls and post-Maintenance Window validations of operationality readiness

- **Hardware/Sizing Estimation (CPU, RAM, disk)**
  - No hardware augmentation is identified due to small processing and storage required if:
    - Assumption Number 4 (a Digital Platform is already deployed) is true
    - Business chooses to leverage the existing EBS infrastructure (but there will be additional labor efforts to re-engineer with custom SAPUI5 screens)

- **Data integration services**
  - Potential integration effort for SAP Records Management (RM) depending on business requirement of DoD 5015.2 standard
  - Does not interface with an external system through middleware

- **Portal integration with existing applications**
  - No Portal integration is identified because there's no existing IT systems to integrate with. If Assumption Number 4 (a Digital Platform is already deployed) is true, Single Sign-On (SSO) solution will already have been developed providing seamless integration and user experience to users so that they only have to provide one credential (CAC card or Username/Password) to be able to access all Digital Platform content authorized by their JD(s)

- **Unstructured data requirements**
  - Unstructured data requirement is identified such as Trace Data that will be uploaded/attached by vendor

- **Lifecycle and Software Dependency**
  - SV-9 – an Information System Component Inventory that tracks application/hardware components (e.g. product names, versions, end-of-support dates, and planned versions). It is reviewed on a monthly basis, and updated based on component installations, removals, and/or updates.
  - Sonatype Nexus – Software Supply Chain Automation which provides the team with ability to continuously manage open-source libraries for safer application development

- **Software License Requirements**
  - No additional license requirements identified if:
    - Assumption Number 4 (a Digital Platform is already deployed) is true
    - Business chooses to leverage the existing EBS infrastructure

10.2.8 Other Considerations

- Additional effort for coordination and migration to DISA DECC-O Production system is needed if Digital Platform is not used
- Coordination with AMPS team and AMPS level of effort is needed for all role updates

10.2.9 Proposed Technical Architecture

The recommended Digital Traceability enhancements will require some integration with current DLA enterprise systems; coupled with providing applicable stakeholders access to relevant components to enable the sharing and analyzing of relevant data. As such, the following technical architecture is proposed to enable the enhancements recommended throughout the document:

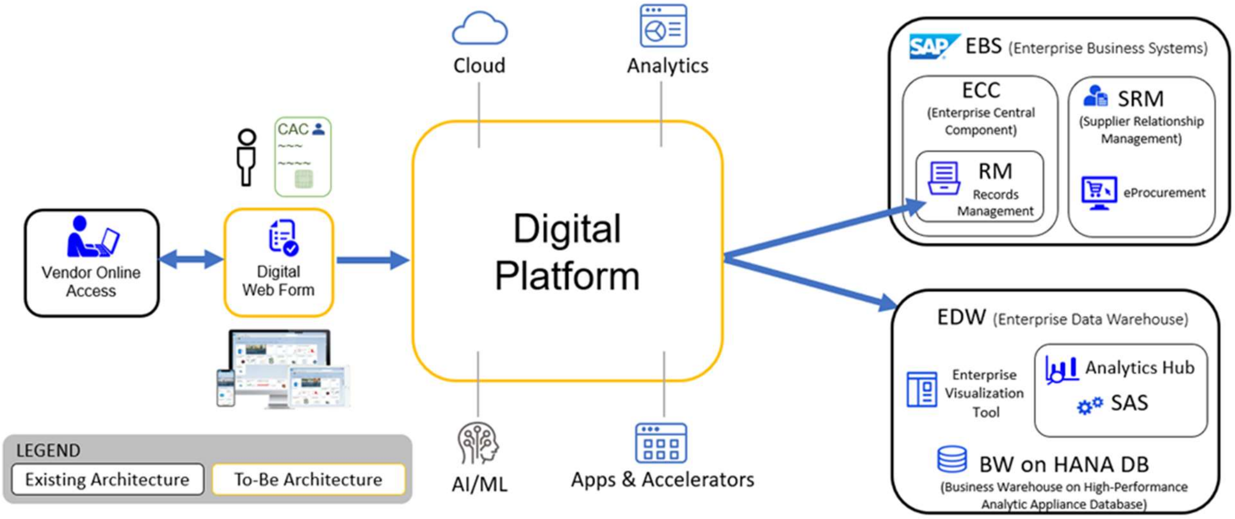

Cloud
Analytics
CAC
Vendor Online Access
Digital Web Form
Digital Platform
AI/ML
Apps & Accelerators
SAP EBS (Enterprise Business Systems)
ECC (Enterprise Central Component)
RM Records Management
SRM (Supplier Relationship Management)
eProcurement
EDW (Enterprise Data Warehouse)
Enterprise Visualization Tool
Analytics Hub
SAS
BW on HANA DB (Business Warehouse on High-Performance Analytic Appliance Database)
LEGEND
Existing Architecture
To-Be Architecture

Figure 43. *Proposed Technical Architecture for Digital Traceability Enhancements*

10.3 EBS Integration Level of Effort

10.3.1 Tech Management Impact

- Portal (iViews/Pages/RolesSSO to new apps)
  - No Portal support required if Digital Platform is used

- PI/Middleware
  - If SAP Records Management (RM) is needed, PI/Middleware support will be required

- BASIS (environment planning and administration)
  - If SAP Records Management (RM) is needed, BASIS support will be required

- Application Security (role updates and creation, user updates and creation)
  - Will likely require updates to existing JD or creation of new JD roles to support new Digital Traceability functionality within EBS.

- Archiving and Retention Management (Data archiving objects and unstructured data storage)
  - Existing Application does not archive data.

- Performance and Stress Testing
  - Performance and Stress Testing (PST) Test Cycles may be necessary if the transaction volume and frequency is large in order to ensure system stability and optimal performance
  - Code Review can be performed for proper coding standards and performance tuning

11.0 Conclusion

The Digital Traceability project analyzed the existing processes in place to collect and review information by the Counterfeit Detection and Avoidance Program, Trade Security Control, and Joint Certification Program. All three programs are integral to the safeguarding of the DLA supply chain by vetting potential business partners during various portions of the procurement process. Detailed analyses found that significant delays exist due primarily to the manual collection and review of requisite information provided by external partners (i.e. vendors, downstream purchasers, etc.). As a means for eliminating many of these delays, web-based data collection, automated validations, enterprise data storage, and business intelligence dashboards have been recommended.

The external data submitted for each program varies in both sensitivity and specificity of required information. As such, detailed recommended requirements were provided for each individual program so that J6 Information Operations may determine an appropriate production design if the enhancements are approved. Additionally, enterprise data storage approaches were recommended and time-saving automation steps such as field-level validation and internal data matching were proposed.

The initial phases of Digital Traceability focused solely on the Counterfeit Detection and Avoidance Program, so additional prototyping and detailed development was performed for that group. A prototype of the digital Form-918 was built and user tested by CDAP resources. Additionally, several business intelligence dashboard views and metrics were built using Qlik Sense to demonstrate reporting capabilities for CDAP leadership. Although Qlik Sense views were not developed for JCP or TSC due to extension timing and funding constraints, both programs expressed interest in similar reporting capabilities.

Finally, a variety of specific technical considerations were documented to give J6 a detailed understanding of existing and future state technical requirements for these programs. Program leaders should collaborate with J6 when determining future state plans and consider combining data interfaces, data storage locations, and reporting capabilities. Overarching program synergies should be explored to provide the best possible future outcomes for the enterprise and supply chain risk management approaches.

APPENDIX: List of Acronyms

ADNAS – Applied DNA Sciences
AMPS – Account Management and Provisioning System
ATO – Authority to Operate
BDA – Business Decision Analytics
BI – Business Intelligence
CAC – Common Access Card
CAGE – Commercial and Government Entity
CCL – Commerce Control List
CDAP – Counterfeit Detection & Avoidance Program
CDD – Contract Delivery Date
CDO – Chief Data Officer
CLIN – Contract Line Item Number
CoC/T - Certificate of Conformance and Traceability
CONOPS – Concept of Operations
COOP – Continuity of Operations Plan
CPU – Central Processing Unit
DCA – Design Control Activity
DCIRS – DLA Criminal Incident Reporting System
DDoS – Dedicated Denial of Service
DDWO – Defense Distribution Warren Ohio
DFARS – Defense Federal Acquisition Regulation Supplement
DIBBS – DLA Internet Bid Board System
DISA – Defense Information Systems Agency
DLA – Defense Logistics Agency
DLAD – Defense Logistics Acquisition Directive
DNA - Deoxyribonucleic Acid
DoC – Department of Commerce
DoD – Department of Defense
DoS – Department of State
DPL – Denied Persons List
DR – Disaster Recovery
DT – Digital Traceability
DUNS – Data Universal Numbering System
DTC – Defense Trade Controls
EBS – Enterprise Business Systems
ECC – Enterprise Central Component
EDW – Enterprise Data Warehouse
EPLS – Excluded Parties List System
ERP – Enterprise Resource Planning
EUC – End-Use Certificate
FAQ – Frequently Asked Questions
FEDRAMP – Federal Risk and Authorization Management Program
FSC – Federal Supply Class
FTE – Full Time Equivalent

GAO - Government Accountability Office
KPI – Key Performance Indicator
ICE – Immigration and Customs Enforcement
IDM – Identity Management
IL – Impact Level
ISCP – Information System Contingency Plan
ISSM – Information System Security Manager
ISSO – Information System Security Office
IT – Information Technology
JCO – Joint Certification Office
JCP – Joint Certification Program
L&M – Land and Maritime
MAC – Mission Assurance Category
MPR – Monthly Progress Reports
NIIN – National Item Identification Number
NIST – National Institute of Standards and Technology
OCM – Original Component Manufacturer
OEM – Original Equipment Manufacturer
OIG – Office of Inspector General
OPM – Office of Personnel Management
PaaS – Platform-as-a-Service
PAR – Post Award Request
PDF – Portable Document Format
PII – Personally Identifiable Information
PO – Purchase Order
PST – Performance and Stress Testing
QUID – Quality Information Database
QML – Qualified Manufacturers List
QPL – Qualified Products List
QSLD - Qualified Supplier List of Distributors
QSLM – Qualified Suppliers List of Manufacturers
QTSL – Qualified Testing Suppliers List
RAM – Random Access Memory
RBAC – Role-Based Access Control
RM – Records Management
RMF – Risk Management Framework
RPO – Recovery Point Objective
RTO – Recovery Time Objective
SAM – System for Awards Management
SCRM – Supply Chain Risk Management
SDR – Supply Discrepancy Report
SID – Service Integration and Delivery
SLA – Service-Level Agreement
SME – Subject Matter Expert
SOD – Segregation of Duties
SOP – Standard Operating Procedure

SPRS – Supplier Performance Retrieval System
SSO – Single Sign-On
TCB – Technical Control Board
TCO – Total Cost of Ownership
TD – Technical Data
TECS - Treasury Enforcement Communication System
TQ – Technical Quality
TSC – Trade Security Control
TSCAO - Trade Security Control Administration Office
UAT – User Acceptance Testing
UI – User Interface
USML – United States Munitions List
UV – Ultraviolet
UX – User Experience
VNMC - Vendor Network Mapping Capability