

REPORT DOCUMENTATION PAGE				<i>Form Approved</i> OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (MM-YYYY) 20220815		2. REPORT TYPE Final		3. DATES COVERED (From - To) 20201001-20220815	
4. TITLE AND SUBTITLE Digital Rights Management for Technical Data Packages				5a. CONTRACT NUMBER SP4701-20-D-9028	
				5b. GRANT NUMBER NA	
				5c. PROGRAM ELEMENT NUMBER NA	
6. AUTHOR(S) Matthew C. Bishof, Jillian E. Clark, Garrikk W. Gibson, Charles J. Lorence, Shannon Marnien, Jenel H. Newton, Jason M. Sheridan, Martin S. Shinko				5d. PROJECT NUMBER NA	
				5e. TASK NUMBER NA	
				5f. WORK UNIT NUMBER NA	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) LMI 7940 Jones Branch Drive Tysons, VA 22102				8. PERFORMING ORGANIZATION REPORT NUMBER NA	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Senthil Arul, Defense Logistics Agency, Defense Logistics Agency 8725 John J. Kingman, Fort Belvoir, VA 22060				10. SPONSOR/MONITOR'S ACRONYM(S) DLA R&D	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) NA	
12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution Statement A Unlimited Public Release					
13. SUPPLEMENTARY NOTES NA					
14. ABSTRACT The current systems used by DLA allow prospective suppliers to download a TDP without ensuring the data cannot be withdrawn or destroyed. In addition, it is difficult to make changes to DLA's existing systems due to a variety of factors, such as cost of changes, competing requirements for limited system change funding, and achieving organizational consensus on change. Using our deep knowledge of DLA's players, processes, and systems, and the results of intensive market research and subject matter expert interviews, LMI developed 51 functional requirements tailored to DLA's unique needs, and evaluated 21 leading commercial digital rights management (DRM) solution providers against these requirements for their potential benefit to DLA. We assessed DRM's ability to enhance DLA's technical data security—while minimizing burden to end-users by exploring the ability of commercial DRM tools and techniques to improve the security of TDPs that DLA is required to provide its suppliers to support competitive procurements. In doing so, LMI determined that EDRM—that is, DRM technologies targeted toward enterprise use cases often related to information access and use—vice consumer DRM more traditionally deployed in the context of streaming media, is well-suited to DLA's specific and unique needs, and stands to enhance DLA's technical data security posture. Notably, while the team also found that blockchain solutions have some promise within the context of a broad EDRM solution, blockchain itself is not a standalone solution.					
15. SUBJECT TERMS Digital Rights Management, Enterprise DRM, Blockchain, Technical Data, Digital Thread, Digital Security, Cybersecurity					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Unclassified Unlimited	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Laura Tyler
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U			19b. TELEPHONE NUMBER (include area code) 703-917-7317



Digital Rights Management to Secure Technical Data Packages

August 2022



Digital Rights Management to Secure Technical Data Packages

Matthew C. Bischof

Jillian E. Clark

Garrick W. Gibson

Charles J. Lorence

Shannon Marnien

Jenel H. Newton

Jason M. Sheridan

Martin S. Shinko

August 2022

NOTICE:

THE VIEWS, OPINIONS, AND FINDINGS CONTAINED IN THIS REPORT ARE THOSE OF LMI AND SHOULD NOT BE CONSTRUED AS AN OFFICIAL AGENCY POSITION, POLICY, OR DECISION, UNLESS SO DESIGNATED BY OTHER OFFICIAL DOCUMENTATION.

LMI ©2022. ALL RIGHTS RESERVED. 11611.004.00L1

Digital Rights Management to Secure Technical Data Packages

August 2022

Executive Summary

The Defense Logistics Agency (DLA) supplies spare parts and other materiel to the military services. To offer these services, DLA consumes technical data packages (TDPs) developed by program offices in the military services that define the materiel that DLA procures. To support procurements, as necessitated by the Office of the Secretary of Defense policy and federal law (the Competition in Contracting Act), DLA must furnish potential suppliers with TDPs that impart enough information for suppliers to submit an authoritative price quote during the solicitation process.

Any entity qualified to do business with DLA should be able to access these TDPs to ensure that DLA places no additional burden on doing business with the federal government. However, once a supplier downloads a TDP, there is no mechanism for withdrawing the data or ensuring that the supplier destroys the data. If suppliers retain information from TDPs, malefactors could obtain large quantities of unclassified but valuable technical data if they gain access to supplier systems.

The current systems used by DLA allow prospective suppliers to download a TDP without ensuring the data cannot be withdrawn or destroyed. In addition, it is difficult to make changes to DLA's existing systems due to a variety of factors, such as cost of changes, competing requirements for limited system change funding, and achieving organizational consensus on change.

Using our deep knowledge of DLA's players, processes, and systems, and the results of intensive market research and subject matter expert interviews, LMI developed 51 functional requirements tailored to DLA's unique needs, and evaluated 21 leading commercial digital rights management (DRM) solution providers against these requirements for their potential benefit to DLA. We assessed DRM's ability to enhance DLA's technical data security—while minimizing burden to end-users by exploring the ability of commercial DRM tools and techniques to improve the security of TDPs that DLA is required to provide its suppliers to support competitive procurements. In doing so, LMI determined that EDRM—that is, DRM technologies targeted toward enterprise use cases often related to information access and use—vice consumer DRM more

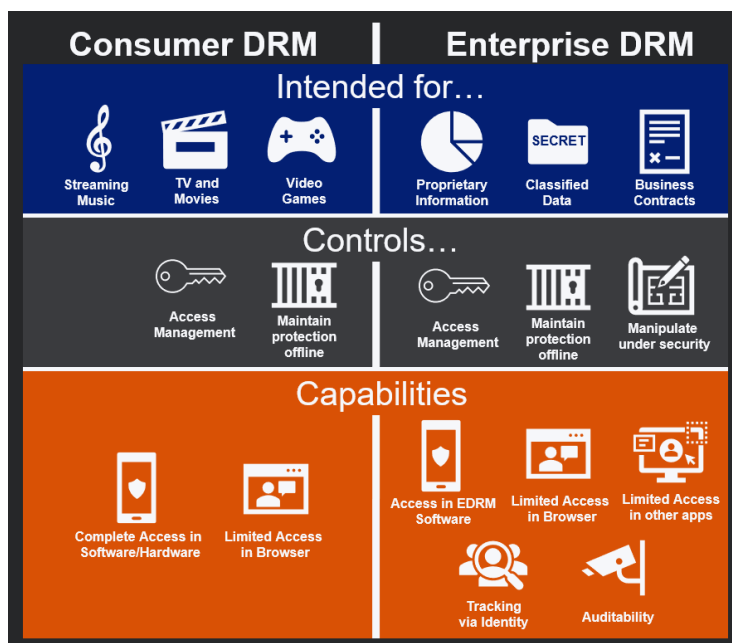
Bottom Line Up Front

LMI found that DLA can better safeguard technical data and its integrity during the procurement process by implementing features of enterprise digital rights management (EDRM).

Using LMI's Transition Plan developed for this project, DLA should apply the results of this analysis to pilot EDRM within their environment, using the 51 DLA-specific technical requirements LMI developed to drive their vendor selection.

traditionally deployed in the context of streaming media (Figure ES-1), is well-suited to DLA's specific and unique needs, and stands to enhance DLA's technical data security posture. Notably, while the team also found that blockchain solutions have some promise within the context of a broad EDRM solution, blockchain itself is not a standalone solution.

Figure ES-1. Consumer vs. EDRM



In light of LMI's findings, DLA should:

- Pursue EDRM solutions to protect its technical data, rather than (consumer) DRM tools and techniques.
- Initiate pilot projects to build on this work within the DLA environment before ultimately selecting an EDRM solution and executing our transition plan to implement said solution at DLA.
- Adopt the 51 technical requirements LMI developed to drive solicitation criteria for commercial solution providers and issue a request for quote accordingly.
- Not pursue blockchain as a standalone solution for managing access to and security of its technical data.

EDRM offers important tools and techniques to DLA's overarching strategic data security posture. In hardening data access and other protections by ensuring that the right data is accessible to the right users at the right time, these tools advance an authoritative source of truth, which in turn seeds a functional and robust digital thread—a key step toward technical data modernization.

Contents

Chapter 1 Introduction	1-1
Background	1-1
Purpose	1-1
Scope	1-2
Approach	1-3
Task 1: Identify Commercial Enterprise DRM Best Practices	1-3
Task 2: Identify Functional Requirements	1-3
Task 3: Develop Test Plan and Evaluation Potential Prototypes	1-3
Task 4: Select COTS Software for Prototypes	1-3
Task 5: Construct Test Hosting Environment for Prototypes	1-4
Task 6: Prototype Execution and Results.....	1-4
Current Method of Securing TDPs at DLA	1-4
Desired Capabilities.....	1-6
Assumptions and Constraints	1-7
Chapter 2 DRM Overview	2-1
DRM and Data Security	2-1
EDRM.....	2-1
Blockchain and EDRM.....	2-2
Chapter 3 Market Research	3-1
Identify Commercial EDRM Best Practices	3-1
Vendor Engagement.....	3-7
Chapter 4 Functional Requirements	4-1
Chapter 5 Prototype Planning and Execution	5-1
Prototyping Test Plan	5-1
Construction of Test Hosting Environment for Prototypes.....	5-1
Selecting the Right Architecture.....	5-2
Prototype Execution.....	5-3
Chapter 6 Findings	6-1
Key Findings.....	6-1
Browser-Only EDRM Solutions Do Not Meet DLA's Needs.....	6-1
EDRM is Compatible with a Model-Based Digital Thread.....	6-1

EDRM is Compatible with CMMC Implications	6-2
EDRM Aligns Well to a Zero Trust Paradigm	6-2
EDRM Performs Well Against DLA-Specific Requirements	6-4
Blockchain Is Not Suitable as a Standalone Solution for DRM	6-4
EDRM Implementation At a Glance: Benefits and Challenges	6-5
Chapter 7 Conclusion	7-1
Appendix A COTS Software Selection	
Appendix B Commercial Best Practices	
Appendix C EDRM Implementation Process Flows	
Appendix D Functional Requirements	
Appendix E Test Plan	
Appendix F Results of Prototype	
Appendix G DRM Requirements Definition	
Appendix H Details Regarding EDRM	
Appendix I Abbreviations	
 Figures	
Figure 1-1. Current Procurement Process at DLA.....	1-5
Figure 2-1. DRM vs. EDRM	2-2
Figure 6-1. Zero Trust Pillars	6-3
 Tables	
Table 1-1. Assumptions and Constraints	1-7
Table 3-1. Vendors Eliminated.....	3-2
Table 3-2. Scored DRM Candidates (I)	3-3
Table 3-3. Scored DRM Candidates (II)	3-4
Table 3-4. Additional Eliminated Candidates.....	3-5
Table 3-5. EDRM Top Candidate Scores.....	3-6
Table 4-1. Baseline and Alternatives	4-1
Table 4-2. COTS Software Selection Criteria.....	4-3
Table 5-1. Test Plan Metrics	5-1
Table 5-2. EC2 Software Configuration.....	5-2

Chapter 1

Introduction

Background

The Defense Logistics Agency (DLA) supplies spare parts and other materiel to the military services. To offer these services, DLA consumes technical data packages (TDPs) developed by program offices in the military services that define the materiel that DLA procures. To support procurements, as necessitated by the Office of the Secretary of Defense policy and federal law (the Competition in Contracting Act), DLA must furnish potential suppliers with TDPs that impart enough information for suppliers to submit an authoritative price quote during the solicitation process.

Any entity qualified to do business with DLA should be able to access these TDPs to ensure that DLA places no additional burden on doing business with the federal government. However, once a supplier downloads a TDP, there is no mechanism for withdrawing the data or ensuring that the supplier destroys the data. If suppliers retain information from TDPs, malefactors could obtain large quantities of unclassified but valuable technical data if they gain access to supplier systems.

The current systems used by DLA allow prospective suppliers to download a TDP without ensuring the data cannot be withdrawn or destroyed. In addition, it is difficult to make changes to DLA's existing systems due to a variety of factors, such as cost of changes, competing requirements for limited system change funding, and achieving organizational consensus on change.

Purpose

In the future, the procurement of replacement parts and the manufacturing processes to supply them will need a digital thread-enabled, three-dimensional (3D) model-based definition and other technical data. Reaching this future state requires careful incremental steps, beginning with ensuring data integrity, managing data distribution, and limiting data flow to authorized partners only.

One technology that controls access and use of content on digital devices to protect data and create confidence in its pedigree is digital rights management (DRM). DRM, at a high level, manages access to digital content via various tools and techniques. Data integrity and distribution control is a necessary precursor for ensuring the cybersecurity of the digital engineering ecosystem, including the model-based enterprise and digital thread that supports distributed applications, such as digital twin and advanced manufacturing technologies.

The purpose of this project is to explore the ability of commercial DRM products and techniques to improve the security of TDPs that DLA is required to provide to its potential suppliers in support of competitive procurements.

Our project considers data access and data integrity. Access tracks who requests, receives, and transfers DLA data as well as when data enters the digital thread. Integrity confirms and ensures that the data arrives and remains intact and unaltered. Another key aspect of any potential DRM solution is to maintain traceability to the authoritative source. DLA must be able to track modifications of its data and derivative products associated with the original data using digital thread technology. This effort tests DRM options that can protect the ongoing development of that digital thread, such that technical data remains secure as it moves from location to location throughout its lifetime.

This project reviewed existing and emerging technologies, standards, and best practices for DRM and evaluated those with value to DLA's environment and requirements, and was constructed around the following tenets:

- DRM is more than cybersecurity.
 - New considerations emerge as DLA works to build the connected digital thread and seeks to maintain an authoritative source of truth.
 - Beyond the systems in use, data itself needs not only to be protected but tracked, similar to an envelope sent via First Class Mail.
- Security needs vary.
 - Technical data changes throughout its lifecycle, from design to manufacturing, validation, etc.
 - Different TDPs have varying security needs.
 - DRM technology accounts for this dynamic environment.
 - Technical data protection hinges on providing the right data to the right users at the right time. DLA needs better visibility and security for technical data that they provide to potential suppliers to avoid misuse of valuable Department of Defense (DoD) technical data.
- DRM is a key component of Technical Data Management Transformation.
 - DRM ensures that authoritative version of the relevant data is the version of the data accessed by selected stakeholders.
 - DRM activity management and logging align with key elements of the model-based enterprise and digital thread, namely the functionality around managing an authoritative version of the data and tracking adjustments and evolution of the data by recorded authors.

Scope

This project involved developing DLA-specific requirements, conducting a detailed market survey of commercial-off-the-shelf (COTS) providers, and developing a prototype to validate the benefits of different DRM techniques and create a foundation for an informed comparison between options for securing technical data. This project also investigated blockchain technology to assess its potential value to DLA alongside DRM.

This project considered solutions that work within and in conjunction with DLA's existing procurement systems, and that do not hinder the exchange of technical data between DLA and suppliers, or detract from the functionality expected by DLA partners and

suppliers. We also considered future cybersecurity posture at DLA and within DoD to ensure the insights gained were valuable over the long term. While building the digital thread was not part of this effort, it remains a consideration for future research and development.

Technologies and processes to prevent unauthorized access and change were within scope, as was furnishing information to the agencies responsible for forensic investigation of when, where, who, and the seriousness regarding data access and use. The forensic investigation itself into the details of the change was out of scope of this project. Prototypes unlikely to result in a viable pilot project were not considered.

Our prototype was designed to be reactive, not preventive—the prototype does not prevent the alteration of technical data, as certain alterations by authorized users are necessary and expected. Rather, the solution prevents unauthorized users from accessing technical data and tracks whether the technical data in question has been altered as well as when, how, and by whom.

Approach

The project team employed the following approach to investigate the marketplace, establish a framework for prototype selection and execution, and catalog results and lessons learned.

Task 1: Identify Commercial Enterprise DRM Best Practices

The research team shall establish an understanding of the key tenants of successful DRM, the distinctions between the various types of DRM, and the baseline practices that are relevant to addressing DLA's concerns around data security and validation around exchanges.

Task 2: Identify Functional Requirements

The research team plans to develop a comprehensive list of functional requirements tailored to DLA's needs and informed by the insights gained during investigations of Enterprise DRM (EDRM).

Task 3: Develop Test Plan and Evaluation Potential Prototypes

To ensure the prototypes provided valuable and complete insights to DLA, a robust Test Plan must be developed to measure the capabilities of the selected prototype(s) against a thorough set of use cases and conditions.

Task 4: Select COTS Software for Prototypes

Using the commercial best practices and baseline of capability requirements generated in Task 1, the team shall select the solution(s) for prototyping from the most relevant and capable commercially available offerings in the marketplace.

Task 5: Construct Test Hosting Environment for Prototypes

A test environment that simulates key characteristics of the DLA's operating environment and processes must be established to evaluate the selected COTS prototype(s) against the functional requirements and Test Plan.

Task 6: Prototype Execution and Results

The selected solution(s) must be tested to assess its suitability and potential for enhancement of DLA business practices around technical data validity and exchange.

Current Method of Securing TDPs at DLA

DLA's current procurement processes do not involve EDRM to control external access to technical data.

EDRM is a distinct branch of the family of technologies within DRM, and became the focus of our research and analysis throughout this project due to EDRM's specific capabilities relative to DLA's unique needs. More information about DRM and EDRM is provided in Chapter 2.

DLA's current procurement process begins when a DoD organization determines it needs to buy a part and initiates a purchase request (PR). Typically, the technical data for parts is provided by the military services' Engineering Support Activities. DLA does not generate this technical data; instead, it uses a standard process for obtaining, consolidating, and making the technical data available in its procurement process. DLA reviews the PR and builds a TDP that includes all relevant information a supplier needs to build or source the part.

After the TDP is completed, DLA prepares a solicitation package and releases it to the public, through the DLA Internet Bid Board System (DIBBS) and its associated "cFolders" site.¹ It is when TDPs are distributed to the public that external access comes into play.

While a two-step authentication process controls access to DIBBS, this access management is not as robust as a potential EDRM solution and captures a much weaker dataset for user and usage analytics.

When supplier companies apply for access, the authentication process includes email verification and a physical address verification step. Although cFolders is accessed via DIBBS, it is a separate system unrelated to DIBBS, so another username registration process is required to access cFolders. Additionally, some data in cFolders require export control certification, foreign secure certification, or licensing agreement certifications before access is granted.

Beyond the steps for obtaining access, there is no mechanism described in DLA materials about DIBBS and cFolders that addresses tracking which users access which data, or dictating what they are allowed to do with that data.

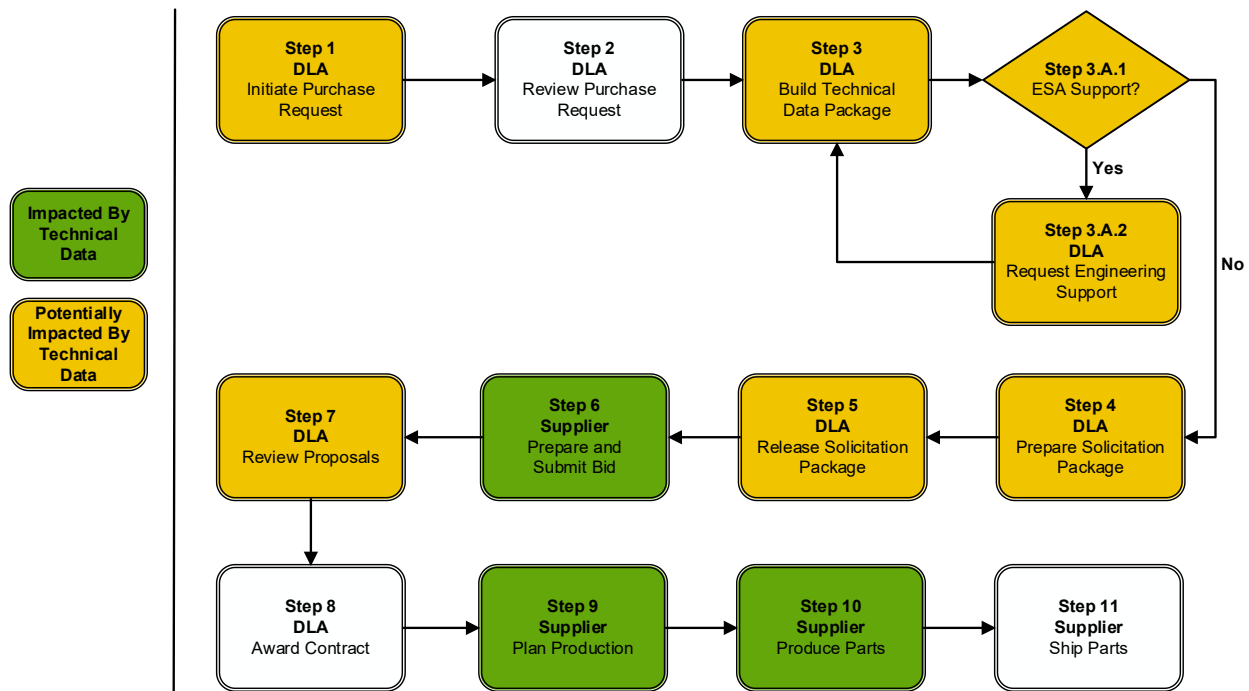
¹ cFolders is the only site that holds technical data intended to be accessed by suppliers.

Suppliers access and review solicitations posted to DIBBS, where they can use an embedded link to view or download the associated TDP in cFolders to facilitate bid and proposal preparation, as well as manufacturing (if awarded a contract).

These suppliers review the solicitation, including the TDP, and prepare quotes and proposals for DLA. DLA then reviews the proposal submissions and awards a contract to the winning supplier. The winning supplier uses the TDP for its planning and to build the part, which it subsequently ships to a designated receiving site.

Figure 1-1 shows DLA's current procurement process. It identifies the entity (DLA or the supplier) that performs each process step and whether the step is affected by the use of technical data (the primary concern is protecting technical data). These steps are repeated for every procurement or acquisition.

Figure 1-1. Current Procurement Process at DLA



Note: This figure is derived from LMI Report DL505T1 Rev. 1, "DLA Can Routinely Procure Parts Using 3D PDF Files," July 2017. ESA = Engineering Support Activity.

Although DLA has control over who can access the portal through which TDPs are downloaded, once files are downloaded and pass through that portal, DLA no longer has any control over them. DLA, the military, and the country rely on the thoroughness of the screening process for who can access the portal—currently the main control method for these sensitive data.

Desired Capabilities

Implementing EDRM can enhance DLA's cybersecurity related to TDPs by enabling the following critical capabilities missing from today's technical data security toolset:

- EDRM solutions provide additional controls beyond the one-time (at download) access controls currently in place at DLA.
- EDRM adds a defensive layer to the individual files themselves. The controls travel with the files, even after files are downloaded. The controls limit the actions on a file based on each user's access privileges and actions.
- Actions are tracked using an audit trail of log entries. Since files cannot be viewed without DLA permission, DLA can control data passed to lower-lever tiers of suppliers in the supply chain.

Implementing EDRM at DLA lays the foundation for data security and for complying with Executive Orders and government policies that continue to focus on the increased protection of data.²

EDRM solutions provide access-tracking features that could allow DLA to track users that downloaded technical data but did not submit a bid. They could allow DLA to track technical data posted but never accessed, to help diagnose issues for parts that receive no offers. This can also allow DLA to flag bids that did not consult the accompanying technical data. Access logging would also enable tracking access attempts of companies that retrieve data outside their areas of historical performance and presumed expertise.

Through access tracking, DLA could also gain insight into their supply chains, such as the subcontractor companies with which suppliers try to partner, because the technical data under EDRM cannot be shared without explicit authorization.

Another potential improvement for the future is using EDRM for offers and proposals submitted by suppliers, protecting bidders and DLA against "man-in-the-middle" cybersecurity attacks, such as by preventing key parameters of proposals from being surreptitiously altered by adverse parties.

² The White House, Executive Order on Improving the Nation's Cybersecurity, May 12, 2021. Accessed June 8, 2022, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

Assumptions and Constraints

Table 1-1. Assumptions and Constraints

Assumptions	Constraints
• The commercial DRM solution we used to build prototypes was representative of DRM solutions available on the broader market. • The mock data provided by DLA is representative of data contained in TDPs.	• We were unable to put sensitive government data into systems that were not pre-approved by the government. While developing our prototypes, we did not import or store any information that was Controlled Unclassified Information (CUI) or greater unless an Authority to Operate existed. • Tracking data 100 percent of the time may not be possible because, in many circumstances, the authorized derivatives necessary to support subordinate processes enter the digital thread. • Some COTS DRM software vendors were unwilling to negotiate the price of their software (Appendix A provides more information about our dealings with specific EDRM vendors).

Chapter 2

DRM Overview

DRM and Data Security

DRM is increasingly important for protecting data, as the abuse of digital content spreads through peer-to-peer file exchanges, torrent sites, and myriad forms of online piracy. DRM allows content creators to protect their copyrighted material and/or intellectual property, safeguard the creative and financial investment they put into their work, and avoid any legal issues that could come from unauthorized use. Using DRM solutions, content creators can:

- Specify and control what other people can and cannot do with their content. This includes restricting or preventing users from editing or saving content, sharing or forwarding products or content, or creating screenshots or screen grabs of content.
- Set an expiration date on documents or media, after which users will no longer be able to access it.
- Lock access only to certain user accounts, Internet Protocol (IP) addresses, locations, or devices, including limiting content to persons in a specific country, such as the U.S.
- Watermark documents to establish ownership and identity.
- Track when, where, and how an individual consumed the media.

DRM also allows organizations to protect themselves from the cybersecurity challenges that all organizations face by putting barriers in place to control access to confidential information, protect customer data, ensure and demonstrate compliance, enhance operational efficiency, and prevent downtime. In addition, DRM technologies make it easier for auditors to investigate and identify leaks. For this reason, DRM is playing a growing role in data security by controlling access to confidential information.

EDRM

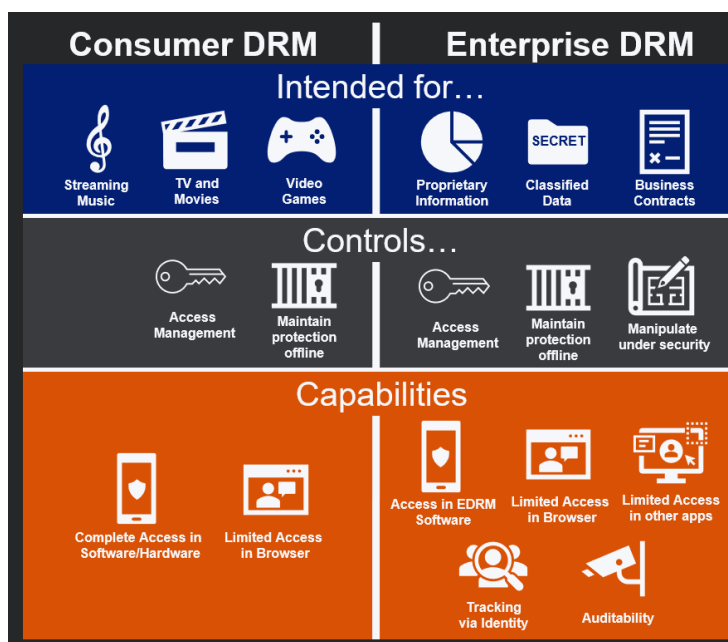
EDRM caters to enterprise use cases, many of which involve protecting sensitive information from unauthorized access and use. Unlike generic DRM that applies to mass-produced media, like music and movies, EDRM applies to documents, spreadsheets, and presentations created by individuals. It allows for sensitive information and data to be created, viewed, modified, and distributed securely, and protects sensitive enterprise information from unauthorized access, use, and distribution by applying rules to the information distributed in electronic documents. Figure 2-1 illustrates the differences between DRM and EDRM at a high level.

EDRM solutions are frequently used to reduce exposure to information risks and prevent data loss when communicating and collaborating with partners. EDRM protects

information against theft, misuse, and inadvertent disclosure and mitigates the business, legal, and regulatory risks of collaboration and information exchanges with partners and customers. For example, an organization might apply EDRM to executive communication to prevent sensitive information from leaking to the media or competitors.

Based on our subject matter experts' (SMEs') findings and knowledge of DLA processes and data environment, EDRM is most applicable to DLA's needs for processing and sharing TDPs (many of which contain sensitive information). For that reason, our efforts focused on EDRM's focused suite of capabilities, rather than broader DRM. The below subsections elaborate on features characteristic of EDRM.

Figure 2-1. DRM vs. EDRM



Blockchain and EDRM

In the course of our overarching research, this project also sought to investigate the use of blockchain technology to implement EDRM. Our research revealed that while blockchain itself is not a DRM solution unto itself, the technology could play a role as part of an EDRM implementation.

A blockchain is usually a digital, distributed ledger of transactions or events, typically decentralized and shared across a peer-to-peer network. It is unique from other electronic ledgers because transactions or events are bundled into “blocks” before being verified and added to the immutable record. The easiest way to conceive of a blockchain is to imagine a ledger that is recording events, like the history in a cash register or an event logger on a personal computer.

More commonly, a blockchain will be decentralized such that every peer has a complete copy of the record, but it is also possible to configure a blockchain to be tightly controlled so that each peer only has a copy of the transactions they participated in. Records on the blockchain are immutable and function in an append-only fashion, designed to prevent any actor (from within or without) from modifying the history of blocks in the chain by making previous blocks an integral part of each new block created. The blockchain grows via consensus of peer nodes.¹ Whether all nodes have equal say or

¹ A node is a participant in the blockchain, such as an individual or organization.

only control nodes manage this consensus, the chain will not grow unless the nodes in power agree to accept the next “block” or bundle of events.

Blockchain, in the EDRM space, can take on a variety of forms. The blockchain could be used to track which users accessed what data, to share and track the keys needed to download said data from the repository, or as a source of truth for data integrity. However, while blockchain may appear to have features in common with EDRM, particularly in preventing unauthorized modification of data, it is not EDRM. In fact, blockchain is designed for public disclosure and every participant gets a copy. Participants can extract data from the blockchain and use it however they like; there is no tracking of how data is used once it is taken (copied) from the blockchain, data cannot be removed from the blockchain, and expired data cannot be deleted from circulation.

A blockchain offers potential for creating immutable records indicating who accessed data, when the access took place, potentially where, and the actions performed. The immutability of the blockchain ensures that the records have not been tampered with and cannot be deleted without glaring indications that modifications took place. The result is a record of activity that can be trusted and used during a forensic investigation.

Chapter 3

Market Research

Identify Commercial EDRM Best Practices

The research team reviewed open-source information describing EDRM best practices as well as several unique sources from government, the commercial sector, and blogs. All sources had overlapping findings, described in Appendix B. These findings were consistent with our SMEs' existing understanding of how to implement EDRM.

We used information from these best practices to influence our EDRM implementation and identify functional requirements and test cases for evaluating EDRM's ability to protect the data within TDPs. This is discussed further in the following section.

Our market research found a broad field of commercial solution providers, with none being dominant in the field. Rather, the market is fragmented, with many participants focusing on DRM to protect streaming video media and software products, and others focused on the EDRM application of securing planning and negotiations related to financial deals such as acquisitions and mergers. Despite the availability of these solutions, the commercial marketplace does not appear to offer the perfect EDRM solution that targets the niche DLA desires.

Materials about commercial products were shrouded by advertising claims that only obliquely hinted at features that were desirable for our prototypes. It appears that the normal marketing approach in this industry is for the potential customer to demonstrate to suppliers that they have funding up front, then work person-to-person with a sales team. Consequently, responding to a government RFP with a firm price offer may be a new and unfamiliar form of doing business for some of EDRM solution providers.

Our initial research efforts identified 21 software vendors who work with or provide DRM services.

- | | | |
|--|---------------------------|---------------------------|
| 1. Adobe Systems Incorporated | 8. Kudelski | 15. Seclore Technologies |
| 2. Apple | 9. Locklizard | 16. Eurostep |
| 3. Box, Inc. | 10. Microsoft Corporation | 17. SIMBA |
| 4. Dell EMC | 11. NextLabs | 18. Vaultize Technologies |
| 5. Fasoo | 12. OpenText | 19. HelpSystems |
| 6. Intertrust Technologies Corporation | 13. Oracle | 20. Verimatix |
| 7. Intralinks | 14. Pimcore | 21. Vitrium Systems |

From the initial list, a deeper dive into the vendors' technologies eliminated nine candidates whose solutions did not meet DLA's minimal needs (a true DRM solution that

accommodates a large set of file types, including computer-aided design (CAD), Adobe PDF, and Microsoft Office). Table 3-1 list the vendors that were eliminated.

Table 3-1. Vendors Eliminated

Vendor	Solution	Description	Link	Exclusion rationale
Apple	HLS (HTTP Live Streaming which Apple uses instead of MPEG-DASH) and FairPlay for encryption	Designed for streaming and sharing media. Not offered as an out-of-the-box (OOTB) solution; you can build your own but not offered as a service.	https://developer.apple.com/streaming/fps/	Apple's Fairplay DRM is explicitly linked to streaming audio/video files and will likely not now or in a future state support DLA's file sharing needs. This is the key objection. Other objections include the restrictions when in the Apple trade space and potential hardware requirements for DoD and supplier partners.
Dell EMC	Virtustream's xStream Management Platform and Infrastructure-as-a-Service (IaaS)	Cloud hosting solution and IaaS offering from an endpoint hardware supplier. Files are secure at rest and in transit but do not provide the tracking tools of other solutions.	https://www.delltechnologies.com/en-ca/collaterals/unauth/offerings-overview-documents/dell-state-and-local-government-solutions-guide.pdf	Does not specifically provide DRM software.
Intralinks	Intralinks UNshare	Niche company for the financial sector.	https://www.intralinks.com/products	Does not appear to accommodate CAD files or manufacturing industry perspectives.
Kudelski	Nagravision	Specializes in providing security for streaming paid content, especially live events and movies.	https://insight.nagra.com/	Streaming only. Does not provide a DRM solution for non-media content.
Locklizard	Locklizard Safeguard PDF DRM Security, Enterprise PDF Security (for Enterprise PDF DRM), Safeguard Secure PDF Viewer	Specializes in PDF copy protection software.	https://www.locklizard.com/digital_rights_management_products/	Limited file types, specifically focused on PDFs.
Microsoft Corporation	Microsoft PlayReady	Must integrate into their app store environment. "Play fair"; is not a service. Not offered as an OOTB solution; you can build your own, but not offered as a service.	https://www.microsoft.com/playready/overview/	Would require a custom implementation, which is beyond the scope of our project. In addition, the software is focused on audio and video copy protection.

Table 3-1. Vendors Eliminated

Vendor	Solution	Description	Link	Exclusion rationale
Oracle	Oracle IRM	Database only. Not offered as an OOTB solution. You can build your own, but not offered as a service.	https://docs.oracle.com/cd/E23943_01/doc.1111/e10724/c05_rights.htm#UCMOV166	Requires installation of Oracle IRM Desktop Client, which communicates back with Oracle IRM Server. Information on the platform was sparse with most documentation being years old. Seems that Oracle IRM is dependent on Oracle Fusion Middleware, Oracles Cloud Platform. These issues of platform adoption requirements in combination with a very limited feature set for DLA's needs compared to other DRM solutions is why it was eliminated.
Seclore Technologies	Seclore Data-Centric Security Platform	Requires data to be moved onto their platform before DRM protections can be applied. Each data file is encrypted security embedded with their document. Focused on the Cybersecurity Maturity Model Certification (CMMC) business.	https://www.seclore.com/digital-rights-management/	Required a very large cost in both consulting and licensing fees to facilitate a prototype for DLA. The cost far exceeded what the project could afford.
Eurostep	ShareAspace	Primarily a document management system geared toward file configuration management.	https://www.eurostep.com/shareaspace-features/	Based upon the vendor's marketing documentation, the system's encryption began and ended with logging into their system. DRM is not implemented on the receiving device.

The remaining 12 candidates were scored against 17 high-level weighted criteria (as shown in Tables 3.2 and 3.3) that comprised the minimum requirements to implement EDRM at DLA. We created these criteria in parallel with our research to establish EDRM best practices and baseline capability requirements for DLA-focused solutions. These criteria were later added to and expanded into 51 functional requirements used to execute the prototype (See Appendix D).

Table 3-2. Scored DRM Candidates (I)

No.	Criteria	Candidates					
		Fasoo	Vera Security	Nextlabs	Simba Chain	Seclore	Intertrust
		Solution rating					
1	Supports relevant filetypes	9	3	9	9	9	9
2	Supports large userbase	9	9	3	9	9	9

Table 3-2. Scored DRM Candidates (I)

No.	Criteria	Candidates					
		Fasoo	Vera Security	Nextlabs	Simba Chain	Seclore	Intertrust
		Solution rating					
3	Can integrate with existing DLA systems	9	9	9	9	9	9
4	Can accommodate existing DLA processes	3	9	9	9	9	9
5	Feasible licensing/pricing structures	1	1	1	9	1	1
6	Performs data delivery verification	9	9	9	9	9	1
7	Offers security for data in transit	9	3	9	9	9	9
8	Data remains in current repositories	9	9	9	9	9	9
9	High ease of use	3	9	9	9	9	9
10	Data access revocation/expiration	9	9	9	9	9	1
11	Baked-in usage tracking/analytics	9	9	9	9	9	3
12	Provides watermarking on data	9	9	9	1	3	1
13	Versioning and version controls	9	3	3	3	3	3
14	Compatible with current processes for DLA's partners	9	9	9	9	9	3
15	Location tracking/logging	9	1	9	9	9	3
16	Desired automation capabilities met	9	3	9	9	9	9
17	Compatible with digital thread	9	9	3	9	3	3
Total score		448	392	436	494	448	344

Table 3-3. Scored DRM Candidates (II)

No.	Criteria	Candidates					
		Box	Vaultize	Vitrium	Pimcore	OpenText	Adobe
		Solution rating					
1	Supports relevant filetypes	3	9	3	9	3	9
2	Supports large userbase	9	9	3	9	9	9
3	Can integrate with existing DLA systems	9	9	9	1	9	3
4	Can accommodate existing DLA processes	3	9	9	3	3	3
5	Feasible licensing/pricing structures	3	1	1	1	1	1
6	Performs data delivery verification	9	9	9	9	9	9
7	Offers security for data in transit	9	9	9	9	9	9
8	Data remains in current repositories	1	9	9	9	9	3
9	High ease of use	3	9	3	9	9	9
10	Data access revocation/expiration	3	9	9	9	9	9
11	Baked-in usage tracking/analytics	9	9	9	9	9	9

Table 3-3. Scored DRM Candidates (II)

No.	Criteria	Candidates					
		Box	Vaultize	Vitrium	Pimcore	OpenText	Adobe
		Solution rating					
12	Provides watermarking on data	9	9	9	9	1	9
13	Versioning and version controls	9	9	9	9	9	9
14	Compatible with current processes for DLA's partners	3	9	3	9	3	3
15	Location tracking/logging	3	9	3	3	1	1
16	Desired automation capabilities met	9	9	9	3	9	9
17	Compatible with digital thread	3	3	3	9	3	3
Total score		448	340	472	382	402	382

The team eliminated an additional seven candidates based on the results of our analysis, reflected on the scorecard (Table 3-4).

Table 3-4. Additional Eliminated Candidates

Vendor	Solution	Description	Link	Exclusion Rationale
Adobe Systems Incorporated	Adobe Experience Manager Assets	Digital Asset Management (DAM) solution primarily focused on image, video, and PDF documents.	https://business.adobe.com/products/experience-manager/assets/features.html	Focus is mostly on the commercial sector and media assets. Files must be moved from their current location and stored within the DAM. Feature set was limited in location tracking and ease of integration into existing DLA systems and processes.
Box, Inc.	Box	Public cloud file management hosting solution that is highly integrated with commercially available applications such as Slack and MS Teams.	https://www.box.com/overview	Appeared to be public cloud only and did not meet our feature set completely (file type limitations, data access revocation limitations, complete reliance on online platform). Required DLA content to be migrated from DLA to Box's cloud hosting solution.
Intertrust Technologies Corporation	ExpressPlay, Intertrust Platform	Focused on video and/or multimedia. Geared toward a media industry.	https://www.intertrust.com/	Too focused on media industry and feature set does not check all our boxes (no watermarking, no data access revocation).

Table 3-4. Additional Eliminated Candidates

Vendor	Solution	Description	Link	Exclusion Rationale
OpenText	OpenText Media Management	DAM software primarily created to help teams and companies organize their digital media for quick location and retrieval. Specializes in searches through the use of metadata tags.	https://www.opentext.com/products-and-solutions/products/customer-experience-management/digital-asset-management/opentext-media-management	Focus is not on protecting digital data. Some limitations in integrating with existing DLA systems and processes. Feature set was not complete (no location tracking, no watermarking). A custom-built solution would be required.
Pimcore	Pimcore Platform	Specializes in data organization. DAM software primarily created to help companies organize their digital assets.	https://pimcore.com/en/platform	Significant limitations in integrating with existing DLA systems and processes. Feature set was not complete (limited location tracking and automation capabilities).
Seclore Technologies	Seclore Data-Centric Security Platform	Requires data to be moved onto their platform before DRM protections can be applied. Each data file is encrypted security embedded with their document. Focused on the CMMC business.	https://www.seclore.com/digital-rights-management/	Required a very large cost in both consulting and licensing fees to facilitate a prototype for DLA. The cost far exceeded what the project could afford.
Vitrium Systems	Vitrium	COTS DRM software.	https://www.vitrium.com/solutions/enterprise-drm	Feature set does not meet some of the basic criteria—userbase size limitation, file type limitations, limited location tracking.

Following our analysis and scoring, and subsequent eliminations, five candidates remained with solutions best-matched to DLA's requirements, as shown in Table 3-5.

Table 3-5. EDRM Top Candidate Scores

Candidate	Scorecard total
Fasoo	448
Nextlabs	436
Seclore	448
Simba Chain	494
Vaultize Technology	472

Based on our analyses against DLA-specific criteria, Fasoo, NextLabs, Seclore, SIMBA Chain, and Vaultize emerged as the top commercial EDRM solution providers. We contacted each of these vendors to obtain more information about their product. With the

exception of SIMBA Chain, all of these five vendors provided us with demonstrations of their software in action. As the sole candidate understanding of the research and development (R&D) nature of this project and willing to adjust cost—otherwise substantial and prohibitive—given those circumstances, LMI selected Fasoo as our prototype.

Vendor Engagement

The responses we received from vendors during the process of selecting a COTS product for our prototypes provided some insights in themselves. Vendor reception seemed somewhat cool, and vendors seemed to want their price structures kept confidential, as though the price could vary depending on what the customer was willing to spend.

Providing a “free sample” offer was typical (e.g., a 2-week free trial completely under the vendor’s auspices) and requesting a longer trial period so that a prototype could be conducted appeared to be an unusual request.

Fasoo was the only vendor who understood the R&D nature of the project and worked to reduce their costs to fit the budget of a short-term proof of concept. Fasoo provided initial group training and several question-and-answer sessions that, while limited in nature, allowed the team to understand and prototype their product. In addition, Fasoo worked with the team to resolve issues that arose during the course of the prototype development process.

NextLabs took the time to fully understand the purpose of the prototype and readied themselves to work with the team and provide access to their software. However, the price of their participation was far more than the project could afford, exceeding our prototype budget by more than an order of magnitude. Attempts to negotiate a lower price could not be resolved, resulting in the team being unable to include the SkyDRM software as a prototype.

Seclore was initially eager to offer their software for prototyping but was unwilling to provide access for a cost lower than a fully licensed commercial price point. Although we explained the small number of users and resources necessary to exercise the proof of concept, Seclore was unwilling to negotiate pricing. Further requests for information concerning their product were met with silence.

SIMBA Chain was a non-starter. Although their web presence suggested they might have a ready-to-deploy DRM solution, it appears they do not provide a DRM product. Instead, the company appears to focus more on providing an Application Programming Interface (API) platform that makes developing software that utilizes blockchain(s) easier. When we contacted them, they suggested utilizing their Automated Data Integrity (ADI) product. Upon further review, the ADI “product” appears to be more of an avenue of investigation for the team: SIMBA Chain’s interest seemed to be in partnering with the team to develop a DRM application. When the team clarified the depth of our R&D budget, SIMBA Chain ceased communication.

Vaultize proved difficult to communicate with. Located in India, the time difference resulted in long lag times of more than 2 or 3 days between email replies. In addition, Vaultize preferred to communicate via WhatsApp, which made it difficult to articulate

messages of lengths longer than one or two sentences. Eventually, the team decided that running a proof of concept with Vaultize would prove too difficult over the life of the prototype.

The prospect of deploying their software in service of DLA and across the Defense Industrial Base seemed irrelevant to the short-term income from a firm purchase to execute a prototype. Non-Disclosure Agreements (NDAs) seemed to be the normal order of business, and these NDAs contained language that prevented the disclosure of product data, such as the results of testing, to anyone. One vendor proposed a purchase order where, after charging LMI for the software, the vendor would own all of LMI's test results such that nothing about the prototype could be reported to DLA without the vendor's permission—in short, the vendor would own any and all materials mentioning its product, including this report. Other vendors set firm prices that were substantially and irreconcilably higher than the scope of this project's budget. Consequently, DLA may find it difficult to attract vendors willing to participate in a pilot project and may further find that in trying to license EDRM software, vendors expect DLA to accommodate their rules.

Appendix A provides more information about our interactions with individual EDRM vendors.

Chapter 4

Functional Requirements

We identified functional requirements based on commercial best practices found in our market research, and by determining a baseline and alternatives reflective of current and potential future DLA processes based on LMI's prior and ongoing work in this space.

Our baseline and alternatives show the movement of TDPs during the procurement process. This enabled us to infer where EDRM would be most useful for protecting the TDP. They are:

- **Baseline:** Current state. A broad RFP distribution of the TDP by DLA with prospective suppliers providing bid packages with TDPs. This scenario describes DLA's current procurement method.
- **Alternative:** Protecting the TDP and validity checks. This involves validated data exchange between DLA and the suppliers.
- **Enhanced Alternative:** Protecting the TDP and monitoring transactions. This involves validated data exchange between DLA and the suppliers and monitoring the events through a logging process.

Table 4-1 provides more details of the baseline and alternatives, showing the movement of a TDP during the procurement process and mapping the sequence of events for each. The process of creating these different states of operations and determining the sequence in which TDPs are processed helped us determine how the EDRM prototype should function when processing TDPs. This, in turn, helped us identify functional requirements and plan for the execution of our testing.

Table 4-1. Baseline and Alternatives

Baseline: Current state. A broad RFP distribution of the TDP by DLA with prospective suppliers providing bid packages with TDPs.	
• Procurement of a manufactured part using current processes. This scenario serves as the baseline of the time and effort to procure a manufactured part and evaluate the level of confidence in the security of the technical data in transit. • The least expensive of the prototypes—uses current production systems and processes. • One-way transfer. The procurement TDP (P-TDP) is available to all requesters as Distribution Statement A.	Sequence of events: 1. DLA advertises the procurement. 2. The TDP and proposal preparation package are made generally available. 3. Prospective bidders trust that the TDP and proposal preparation package are valid and have not been altered.

Table 4-1. Baseline and Alternatives

Alternative: Protecting the TDP and applying validity checks. Involves validated data exchange between DLA and the suppliers.	
- Commercial DRM technology. The DRM solution is an available commercial product rather than specially designed, custom-developed software. - CUI. While information may be controlled, e.g., subject to export controls, its unauthorized disclosure would not reasonably be expected to damage national security (i.e., information classified as confidential). - Suppliers may suggest alternatives and transmit those proposals back to DLA as new DRM protected TDPs containing their IP.	Sequence of events: - DLA advertises the procurement. - The TDP and proposal preparation package are made generally available under DRM protections. - DRM software validates that the TDP and proposal preparation package are valid and have not been altered after data exchanged with potential bidders/suppliers. - DRM software validates supplier data shared back to DLA under DRM protections.
Enhanced Alternative: Protecting the TDP, validated data exchange between DLA and the suppliers, and monitoring the events through a logging process.	
- Commercial DRM technology. The DRM solution is an available commercial product rather than specially designed, custom-developed software. - Commercial digital ledger technology. Traceability of which data were provided to whom and when, recorded using an available, possibly non-centralized, commercial transaction ledger product. - CUI. While the information may be controlled (e.g., subject to export controls), its unauthorized disclosure would not reasonably be expected to damage national security (i.e., information classified as confidential). - Suppliers may suggest alternatives and transmit those proposals back to DLA as new DRM protected TDPs containing their IP. - Suppliers may have limited use when accessing TDP data. Potentially bidders may be limited to view only. Contracted suppliers may have view and use access. - Suppliers may have limited window of time to access TDP data. After time period elapsed or at DLA discretion, access can be revoked.	Sequence of events: - DLA advertises the procurement. - The TDP and proposal preparation package are made generally available under DRM protections. - DRM software validates that the TDP and proposal preparation package are valid and have not been altered after data exchanged with potential bidders/suppliers. - Access to TDPs may be limited based on phase of acquisition or supplier identity. - Access and actions applied to TDPs are logged and monitored. Potential bidder/supplier access can be revoked by DLA. - DRM software validates supplier data shared back to DLA under DRM protections.

Validation of the TDP for tampering is performed during each exchange and proof of safe transfer is sent to DLA.

Validation of the path of the data and validation that changes were authorized is performed during each exchange and proof of safe transfer is sent to DLA.

For more information about the implementation of EDRM, refer to the process flows developed in Appendix C. These process flows focus on the movement and storage of TDP during the procurement process, identifying where EDRM technology can protect data during transit and at rest. Appendix D shows the 51 functional requirements and Appendix E contains the Test Plan used for prototype evaluations. The requirements list includes, but is not limited to, all EDRM commercial best practices identified in our research. The Test Plan focuses on these requirements and capabilities to investigate in the EDRM solution(s) selected.

Our SMEs developed 17 high-level criteria to reduce the list of 12 candidates down to the top 5. These criteria accounted for minimum requirements to implement EDRM at DLA. Criteria weights applied priority rankings and a scoring scale to characterize how well a given solution satisfied the criteria.

Table 4-23 shows these 17 criteria. Appendix A provides the full scorecards that assigned scores (1–5) to individual criteria. Individual candidate scoring can be found within the Market Research section.

Table 4-2. COTS Software Selection Criteria

Number	Criteria	Weight
1	Supports relevant filetypes	5
2	Supports large userbase	4
3	Can integrate with existing DLA systems	5
4	Can accommodate existing DLA processes	4
5	Feasible licensing/pricing structures	4
6	Performs data delivery verification	5
7	Offers security for data in transit	5
8	Data remains in current repositories	4
9	High ease of use	3
10	Data access revocation/expiration	3
11	Baked-in usage tracking/analytics	3
12	Provides watermarking on data	2
13	Versioning and version controls	2
14	Compatible with current processes for DLA's partners	2
15	Location tracking/logging	1
16	Desired automation capabilities met	3
17	Compatible with digital thread	3

Chapter 5

Prototype Planning and Execution

Prototyping Test Plan

The prototype Test Plan is organized around six tasks, shown in Table 5-1. Each contains various test case sets¹ and corresponding actions and sub-tasks that served as evaluation metrics to help our SMEs evaluate the suitability of EDRM for DLA. There are a total of 176 sub-tasks and tasks in the full list of Test Cases (found in Appendix E—Test Cases), and our SMEs systematically evaluated the ability of the prototype to achieve each one in a series of test cases identified in the plan. Each test case set maps to one or more of our 51 requirements and expands on each requirement by testing the requirement from several angles, highlighting limitations and advantages when considering EDRM in DLA’s environment.

Table 5-1 shows the number of tasks, test case sets, and actions and sub-tasks in our Test Plan.

Table 5-1. Test Plan Metrics

Task number	Task title	Number of test case sets	Number of actions and sub-tasks
1	Transfer data to many users securely	5	57
2	Transfer data securely in reverse	2	21
3	Transfer data securely with validity checks	1	8
4	Transfer data securely in reverse with validity checks	1	26
5	Collect forensic information and check the identity of the recipient	8	59
6	EDRM software information	1	5

Appendix E also provides the results of our testers’ evaluations against the tests found within the Test Cases.

Construction of Test Hosting Environment for Prototypes

The team used Amazon Web Services (AWS) to construct a test hosting environment for our prototypes and instantiated four Elastic Compute Clouds (EC2s)—virtual machines/remote computers that users log in to. We then installed software to run the test cases, as shown in Table 5-2.

¹ A test case set refers to two or more test cases.

Table 5-2. EC2 Software Configuration

Type	Name
Operating System (OS)	Windows Server 2016
Browser	Google Chrome
Browser	Microsoft Edge
Office Suite	Microsoft Office 2016 • Word • Excel • PowerPoint • Outlook
CAD	Fusion 360 7.0
PDF Viewer	Adobe Reader DC 2021
Compression	7-Zip 12.02
Network Protocol Analyzer	Wireshark 3.4.7

As previously discussed, we selected Fasoo for the prototyping phase of this project. Their software deployment required a local client module that ensured the user was always governed by the EDRM policies, requiring the user to validate their identity immediately after logging in to Windows. We found that CAD data is not a typical application for EDRM solutions. We came to expect a significant learning curve; what seemed straightforward in documentation could have surprising complexities found by trial and error. Fasoo’s focus on MS Office file formats rather than modern CAD software vendor support complicated our prototyping efforts, but it was clear that this is an area that Fasoo is actively developing as a feature set, with some basic compatibility and workarounds already available.

In order to access a policy server at the vendor’s site (the only alternative available in our prototyping arrangement), we had to open Internet communication ports normally closed against network intrusions. Discussions with the vendor revealed that alternatives were available but were outside of this prototype budget.

Working offline posed a challenge. Although the product we prototyped was supposed to have this capability, it did not function as expected or according to the vendor-supplied documentation. It is possible that the vendor had additional software modules that were not available to us due to our prototype price point, but offline operation was largely not a feature we were able to explore in-depth. We also discovered a “missing module” problem when we tried testing capabilities for securing printing and using watermarks which speaks to the granular feature toggling nature of Fasoo as a product

Selecting the Right Architecture

During our research, we discovered that browser-only-based EDRM solutions—which only allow files to be accessed through a browser—do not meet DLA’s needs. These solutions are distinct from EDRM solutions that use a locally installed client application. Since several of DLA’s use cases involve suppliers using TDP contents within their native applications, browser-only EDRM solutions are unsuitable unless the software allows the TDP to be downloaded, in which case all protections are removed from the

data, thereby defeating the purpose of EDRM. Appendix A provides more information about browser-only EDRM.

Finally, some features of interest, such as a separate validity indicator, seem to have very limited availability in the commercial marketplace at present.

Prototype Execution

Fasoo provided live training and documentation to the team on the use of their software as both a standard user and Fasoo Administrator. Using the provided documentation and training, we configured Fasoo policies to govern test user access during the prototype and executed the extensive list of test cases (see Appendix E for the test cases).

We evaluated the Fasoo prototype for its ability to improve the security of TDPs by assessing the software against each of the test case sets outlined in the Test Cases, documenting the extent to which they satisfied each test. A comprehensive catalog of Fasoo's performance and the prototype's findings are provided in Appendix G.

Chapter 6

Findings

Key Findings

Below are the notable findings and lessons learned associated with EDRM. These findings are the result of both extensive research and the robust prototype of an EDRM solution, as well as work done directly with the mentioned blockchain technologies.

Browser-Only EDRM Solutions Do Not Meet DLA's Needs

Another key concern for DLA is the adoption rate of any new technology or the burden associated with implementing new software requirements on its partners. DLA has a keen interest in low-barrier-to-entry solutions for new security requirements such as Microsoft Office filetypes and Adobe PDFs. Another example is in-browser solutions that only require a modern browser to be installed on partner systems, which is unlikely to impose undue burden. These solutions generally do not require DLA's partners to invest in or adopt any additional resources (hardware or software) to interact with DLA's information and business processes, decreasing the barrier to entry for those attempting to do business with DLA.

Browser-only-based EDRM solutions—which only allow files to be accessed through a browser—do not meet DLA's needs. These solutions are distinct from EDRM solutions that use a locally installed client application. Since several of DLA's use cases involve suppliers using TDP contents within their native applications, browser-only EDRM solutions are unsuitable unless the software allows the TDP to be downloaded, in which case all protections are removed from the data, thereby defeating the purpose of EDRM. Appendix A provides more information about browser-only EDRM.

EDRM is Compatible with a Model-Based Digital Thread

For the purposes of this project, we define “digital thread” as “a network of connections between data representations across data repositories. Data representations could be transmitted unaltered, or data could undergo a transformation somewhere along the digital thread.”¹ The digital thread embodies the connections between data at rest, and the connections can exist whether the data is encrypted, protected, or left unsecured. The digital thread and its multiple data representations are necessary to support all aspects of system and component engineering across a product's lifecycle.

EDRM can be used to protect the digital thread's data at rest and in transit between its repositories, when stored and transmitted in file format. EDRM does not impede the digital thread process but is instead a separate domain compatible with the digital thread concept. It is important to note that EDRM can protect data but cannot create a digital thread or link data to an existing digital thread.

¹ LMI Report “3D Technical Data Solutions,” May 2021, Appendix K.

EDRM is Compatible with CMMC Implications

The DoD is currently implementing another cybersecurity initiative, rolling out CMMC requirements to implement the rule in Defense Acquisition Regulation Supplement 252.204-7019, effective on November 30, 2020.

CMMC 1.0 is divided into 5 levels and involves assessing some 171 cybersecurity practices in 17 domains like access control, awareness and training, media protection, and security assessment. At its lowest level, it measures organizations' incorporation of basic cybersecurity practices, such as limiting physical access only to authorized individuals and escorting visitors. In general, there is limited overlap between CMMC practices and EDRM capabilities and implementing EDRM can satisfy some CMMC practices. For example, the level of fine-grained control possible when using EDRM, which controls data while in use and at rest, fulfills and goes well beyond CMMC practice "SC.3.191, Protect the confidentiality of controlled unclassified information at rest."²

CMMC 1.0 was planned to apply to all DLA solicitations and contract actions beginning in October 2025. Full implementation of CMMC requires cybersecurity audits conducted by certified independent third-party organizations. Audits are to be conducted using National Institute of Standards and Technology (NIST) Special Publication 800-171.³ Because full implementation goes well beyond self-assessments envisioned in the initial CMMC plans from 2020,⁴ DLA embarked on pilot project efforts to accomplish a phased implementation of CMMC beginning in FY21 through the full implementation in FY26. DLA planned to identify pilot acquisitions in varying quantities. For example, DLA is targeting only 1 acquisition in FY21, which would have increased to 32 in FY25.⁵

EDRM can work hand-in-hand with the implementation of CMMC mandates by preventing the inadvertent disclosure of protected data as well as insider disclosure of such data. However, the exact CMMC practices satisfied by EDRM are yet to be determined.

EDRM Aligns Well to a Zero Trust Paradigm

The DoD is currently implementing another cybersecurity initiative, investing resources in establishing a Zero Trust Architecture and Methodology DoD-wide via the products out of the DoD Zero Trust Portfolio Management Office (ZT PfMO). See National Manager Memorandum 2022-01: National Security Memorandum 8, Zero Trust Security and Cloud Migration Security Guidance, February 2, 2022 and Executive Order 14028 on Improving the Nation's Cybersecurity, May 12, 2021.

EDRM has the ability to strengthen multiple pillars of the Zero Trust framework currently being developed by the ZT PfMO. "Zero Trust is not a capability or device you buy, rather it is a security framework, an architectural approach, and a methodology to

² Office of the Undersecretary of Defense, Acquisition and Sustainment, CMMC, Version 1.02. March 18, 2020. Accessed June 23, 2022, https://exostar.b-cdn.net/inc/uploads/2020/05/CMMC_ModelMain_V1.02_20200318.pdf.

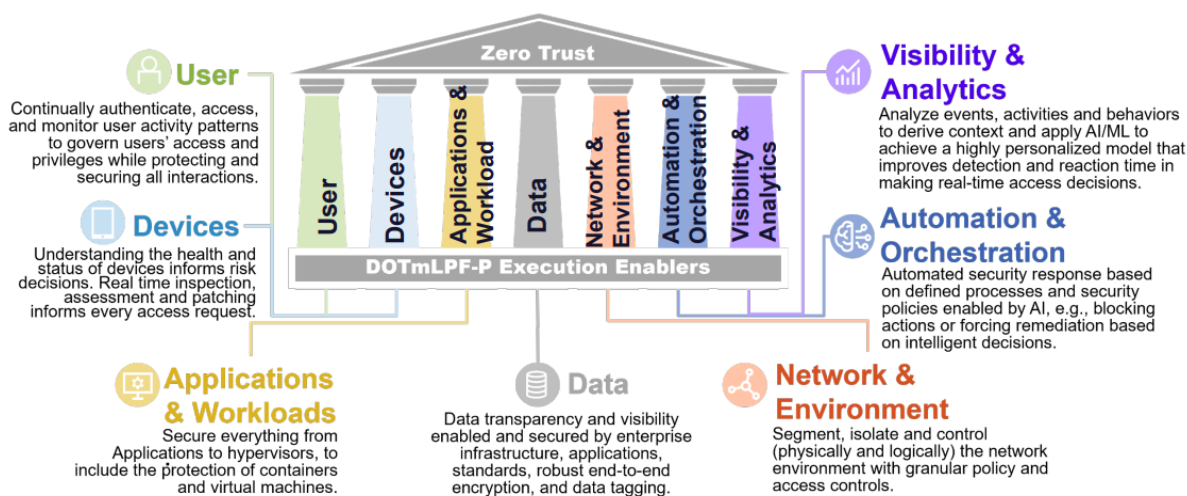
³ NIST, NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, accessed June 17, 2022, <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>.

⁴ U.S. Government, Interim Rule 2019 D041, Assessing Contractor Implementation of Cybersecurity Requirements, accessed June 17, 2022, <https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of>.

⁵ DLA, "CMMC Notice," file accessed June 17, 2022, <https://www.dla.mil/Portals/104/Documents/InformationOperations/EBS%20Supplier%20Information/CMMC%20Notice.docx?ver=IL5zRPt82RWDufAynrbD7A%3d%3d> accessed June 14, 2022.

prevent malicious actors from accessing our most critical assets and reducing existing attack surfaces”—Mr. Randy Resnick, Director, DoD ZT PfMO. EDRM is a suite of capabilities which can be implemented to support this framework and enhance the methodologies around data centric security. Figure 6-1 contains the Zero Trust Pillars.

Figure 6-1. Zero Trust Pillars



Source: Zero Trust – The Time is Now! Tim Denman, DoD Zero Trust Portfolio Management Office (ZT PfMO) Presented by CSIAC Webinar, 7/20/22.
https://lmigov.sharepoint.us/sites/11611004/Project%20Documents/Working/Research/Zero_Trust/Denman-ZT-Presentation-CSIAC-July-2022-v-3.pptx-Read-Only-1.pdf.

Note: AI = artificial intelligence; ML = machine learning.

EDRM addresses most of these pillars in the following ways:

- **Users:** EDRM provides functionality around user authorization for data
- **Devices:** EDRM can restrict access to protected data to devices with specific security profiles
- **Applications and Workloads:** EDRM can control and limit functionality of software applications manipulating protected data.
- **Visibility and Analytics:** EDRM captures information that can be used in analytics and forensics around data security.
- **Automation and Orchestration:** EDRM can automatically withdraw access to data based on time limits or other criteria, securing information without human intervention.
- **Data:** EDRM provides robust encryption and data tagging.

EDRM is not the only enterprise enhancement necessary to adopt the Zero Trust framework, but it addresses multiple facets of the initiative and does not conflict with the overall paradigm shift, making it an excellent technology and investment as Zero Trust becomes standard practice across the DoD.

EDRM Performs Well Against DLA-Specific Requirements

Of the 51 EDRM suitability requirements for DLA, the software completely satisfies 32 (63 percent) of them and partially satisfies 9 (18 percent). That is, the software satisfies 81 percent of requirements at least partially. We believe this indicates that DLA should pursue an EDRM solution to protect its technical data. The requirements and prototype results are documented in Appendix D.

Blockchain Is Not Suitable as a Standalone Solution for DRM

While blockchain may appear to have features in common with DRM, particularly for preventing unauthorized modification of data, it is not DRM. Blockchain is designed for public disclosure: every participant gets a copy. Participants in the blockchain can extract data from the blockchain and use it however they like. There is no tracking of how data is used once it is taken (copied) from the blockchain.

Two of the biggest advantages of blockchain are its ability to function in a trustless environment by utilizing a consensus algorithm such as proof of work or proof of stake, and the decentralized nature of each peer node having a complete copy of the record. Neither of these advantages are appropriate for DLA's needs, as a trustless, open peer-to-peer history of DLA's business transactions will not be an option. While blockchains can be configured as private, a federated permissioned blockchain is very similar to a standard digital ledger in terms of function, and security and efficiency may even be less performant.

The most applicable configuration of a blockchain for the DLA is to assist in securing TDPs alongside other EDRM controls. This can be accomplished as a centralized and trustless (federated and permissioned) blockchain, where the immutable quality of records stored on a blockchain would be most beneficial to DLA. A traditional digital ledger can be modified by a malefactor who gained unwarranted access, and without strong cybersecurity protocols to prevent loss of the true record, such a breach could cause irreparable harm to DLA operations. With the immutable ledger component of a blockchain as a central source of unmodifiable truth to validate authenticity, DLA can guarantee the cryptographic validity of both access records on the chain and content of the files themselves through comparing stored (also on the chain) checksum hashes.

While traditional blockchain platforms are generally dedicated to tasks like cryptocurrency, automating enterprise business actions, and digitizing business artifacts (e.g., contracts), DRM-focused blockchain is less common and largely untested. Applications and technologies that use the underlying data structures and concepts of blockchain are more applicable to the DLA's EDRM use case. One such example is Amazon's Quantum Ledger Database (QLDB).

Amazon QLDB is closer to a traditional data store but with a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log owned by a central trusted authority (i.e., blockchain). Amazon QLDB tracks and maintains a complete and verifiable history of changes over time in an append-only blockchain structure and is faster than traditional blockchain frameworks because it does not incorporate the peer-to-peer consensus algorithms that are resource intensive. It uses familiar SQL-like operators and a document data model for handling

transactions and could function as the server-side read-write data source of a verification and validation step in a larger EDRM workflow.

EDRM Implementation At a Glance: Benefits and Challenges

Benefits when implementing an EDRM solution at DLA include:

- Immediately enhancing the cybersecurity posture of DLA's internal and external file exchange.
- Offering new capabilities to control who can access the contents of a file and the actions they can take, even outside of DLA's enterprise IT systems.
- Supports most filetypes and their native applications, i.e., MS Office, Adobe Acrobat PDF, etc.
- Offers a low impact on DLA's internal practices. The organization can continue using the standard software currently in use, store files in the same locations, and continue sharing those files in the same manner.
- Provides forensic information, including who did what, when they did it, and where, captured as log entries for review if necessary.

Challenges when implementing an EDRM solution include:

- Likely requires suppliers to install a version of the EDRM software on their own devices to enable access to protected files. There may be pushback from industry to such a requirement.
- Limited ability to securely display data within a web browser, but the ability to edit those files is severely limited, especially regarding technical data.
- Unlikely to support all CAD software applications in one. Accessing a CAD file using unsupported CAD software would require the supplier to remove EDRM protection before using the file.
- In addition to installing the client, DLA will need to manage the accounts assigned to suppliers. Given the large number of suppliers DLA works with during any given year, managing accounts may become a fulltime job for DLA employees or hired consultant services.

Chapter 7

Conclusion

This project demonstrated that EDRM can help protect DLA's TDPs at rest, in transit, and in use. This project provides DLA with information for what it can expect from vendors in terms of meeting its requirements for document security, and how EDRM can be used in DLA.

To best illustrate the impact of EDRM, we need to revisit the metaphor selected to describe DRM technology at the onset of this study: a sealed envelope. When one puts a letter, a check, or other important document into an envelope and seals it, the expectation is that your document is routed efficiently, arrives at the selected destination intact, is still sealed in the same envelope, and has yet to be accessed by anyone prior to its arrival. The guarantees of the U.S. Postal Service are familiar and generally trusted. A comparable digital capability was sought because DLA sends thousands of documents a year to its trusted partners and wants to ensure they are only sharing the right information with the right people.



The same assurances when sharing important digital files is of great value to DLA as it shares technical data throughout the defense industrial base. Any technology that could put technical data into a safe container and ensure that the data DLA sent is the same as the data that arrives would only enhance the cybersecurity mission of DLA and DoD as a whole. EDRM technologies offer this kind of assurance and go beyond the envelope analogy. Not only does this technology protect DLA's information on a file-by-file basis, but it can also control and monitor access outside of the DLA IT enterprise.

Sharing data across the Internet is also not exactly like sending information through the mail. When these secured (EDRM-encrypted) files are sent through the Internet, the information is not put into a single envelop so much as every bit of data is split into a cache of separate envelopes. When this bundle of envelopes is "mailed" online, instead of a single stream of data being routed through nodes along a set path, the file is divided into packets and each packet is routed separately across the network. Combined with encryption, this makes it statistically unlikely for a malicious actor who manages to intercept the mail from comprehending what it is they stole. Then, when designated partners receive their bundle of protected data, the packets are assembled in the correct order and the EDRM solution on their end unseals each envelope, securely rebuilding the file for their use.



But EDRM goes further, controlling these envelopes to prevent DLA partners from doing more than just viewing the file. It can add watermarks with user information to identify the recipient, prevent screen captures, and prevent creating copies. Notifications can be automatically delivered to DLA when the files are received and when they are accessed—and often who accessed the files. And should DLA decide that partner access to the data is no longer necessary, the envelopes can be locked down, preventing further access or use until otherwise directed.



The envelope analogy originally used to describe the functionality of DRM to DLA can therefore be expanded: it is not one sealed envelope, but many packets of data sent across the Internet, all individually sealed and scrambled to prevent malicious actors from intercepting sensitive information. The envelope's utility does not end when it is opened but continues to report on data usage and offer enhanced security even beyond the enterprise of DLA.

Based on our findings, DLA should take steps to:

- Pursue EDRM solutions to protect its technical data, rather than (consumer) DRM tools and techniques.
- Initiate pilot projects to build on this work within the DLA environment before ultimately selecting an EDRM solution and executing our transition plan to implement said solution at DLA.
- Adopt the 51 technical requirements LMI developed to drive solicitation criteria for commercial solution providers and issue a request for quote accordingly.
- Not pursue blockchain as a standalone solution for managing access to and security of its technical data.

EDRM offers important tools and techniques to DLA's overarching strategic data security posture. In hardening data access and other protections by ensuring that the right data is accessible to the right users at the right time, these tools advance an authoritative

source of truth, which in turn seeds a functional and robust digital thread—a key step toward technical data modernization.

Following selection of the best EDRM solution to address the 51 requirements developed by the LMI project team, we recommend a review and implementation of the attached Transition Plan. A comprehensive and focused transition is key to the success of the EDRM transition and onboarding of partners.

LMI has established that DLA can take meaningful steps toward simultaneously enhancing the accessibility and security of its procurement technical data in transit. As DLA, and DoD, continue to implement a digital engineering framework rooted in the Model-Based Enterprise and Digital Thread, adopting an EDRM-based approach to data protection substantially moves the needle toward a secure, authoritative procurement data stream that furthers DoD's strategic goals and enhances warfighter readiness.

Appendix A

COTS Software Selection

During our market research, we compared EDM technologies using the 17 criteria listed in Table A-1. Each criterion is prioritized with a value from 1 to 5, with 5 being the highest priority. Each technology is scored on its effectiveness for each criterion. The scores are listed to the right of each criterion under the Priority Weighting Assumptions column.

Table A-1. COTS Software Selection Criteria

Number	Criteria	Priority	Scoring scale
1	Supports relevant filetypes	5	9 = platform is designed to facilitate the sharing and security of relevant filetypes of relevant sizes 3 = platform is able to share a wide variety of file types and large file sizes and can be customized 1 = platform can share limited filetypes of limited sizes
2	Supports large userbase	4	9 = scaling up the platform to meet DLAs needs would not pose a significant challenge 3 = scaling up platform capacity to meet DLA's needs would require innovation 1 = platform might be able to support DLA's needs with significant innovation and retooling
3	Can integrate with existing DLA systems	5	9 = platform can easily pair with DLA's existing enterprise systems and is already FedRAMP approved, 3 = platform can pair with DLA's existing enterprise systems but requires an audit to gain necessary federal security certs 1 = platform may be able to pair with DLA's enterprise systems given significant retooling, the platform requires an audit to gain necessary federal security certs
4	Can accommodate existing DLA processes	4	9 = will not significantly impact DLA processes and operations 3 = will moderately impact DLA processes and operations 1 = will significantly impact DLA processes and operations
5	Feasible licensing/pricing structures	4	9 = platform already has pricing structures in place for the scale of DLA operations which accommodate DLA's needs and these prices are reasonable and non-burdensome 3 = platform already has pricing structures in place for the scale of DLA operations but prices are high 1 = platform has no pricing structures in place for the scale of DLA operations and userbase
6	Performs data delivery verification	5	9 = key, baked in function of platform is data delivery verification 3 = functionality to allow data delivery verification is possible in the platform 1 = secondary technology would be required to enable data delivery verification

Table A-1. COTS Software Selection Criteria

Number	Criteria	Priority	Scoring scale
7	Offers security for data in transit	5	9 = platform defends data in transit and offers DLA forensics on security post-transfer 3 = platform offers DLA forensics on security post-transfer 1 = secondary technology would be required to enable security in transit
8	Data remains in current repositories	4	9 = platform integrates with DLA's current data repositories, acting only as conduit 1 = platform requires data be relocated into new repository (at least a copy of the data)
9	High ease of use	3	9 = platform presents hardly any change to existing DLA user's workflow 3 = platform presents a user-friendly, low learning curve for DLA workers 1 = platform has a steep learning curve for DLA workers
10	Data access revocation/expiration	3	9 = platform is designed to track and control user access 3 = platform can be used to track user access and give DLA the ability to control it 1 = platform does not offer a way to track or modify user access to shared data
11	Baked-in usage tracking/ analytics	3	9 = platform is designed to track user behaviors for analytics 3 = platform can be used to track user behaviors for external analytics 1 = platform does not offer a way to track or user behaviors
12	Provides watermarking on data	2	9 = platform offers feature to watermark/somehow tag data 1 = secondary software required to watermark/somehow tag data
13	Versioning and version controls	2	9 = platform has native features to track versions of data and log changes as well as provide authoritative source of truth 3 = platform can be used to ensure authoritative single source is not changed 1 = platform does not support versioning or authoritative source controls
14	Compatible with current processes for DLA's partners	2	9 = platform presents hardly any change to systems/ workflows of DLA partners 3 = platform presents a user-friendly, low learning curve for DLA's vendor partners and moderate changes to system requirements 1 = platform has a steep learning curve for DLA's vendor partners and major compliance restrictions
15	Location tracking/logging	1	9 = key feature platform can track location of DLA data/ user access 3 = platform logs data which can be used to track location of DLA data/user access 1 = secondary software can be used to track location of DLA data/user access

Table A-1. COTS Software Selection Criteria

Number	Criteria	Priority	Scoring scale
16	Desired automation capabilities met	3	9 = platform enables DLA to fully automate low-level processes with minimal support from staff 3 = platform enables DLA to automate low-level processes with moderate support from staff 1 = platform makes automation difficult/significant number of manual processes remain for DLA staff
17	Compatible with digital thread	3	9 = platform compatible with enabling a digital thread should DLA and vendors update to a model-based environment 1 = the platform restricts ability to achieve a digital thread or a model-based environment

We then met with vendors to determine how suitable each product was for serving as our prototype and excluded many from the project.

Table A-2 shows these 21, and our rationale for excluding them from the project, as applicable.

Table A-2. COTS DRM Software

Vendor	Solution	Description	Link	Exclusion rationale
Adobe Systems Incorporated	Adobe Experience Manager Assets	DAM solution primarily focused on image, video, and PDF documents.	https://business.adobe.com/products/experience-manager/assets/features.html	Focus is mostly on the commercial sector and media assets. Files must be moved from their current location and stored within the DAM. Feature set was limited in location tracking and ease of integration into existing DLA systems and processes.
Apple	HLS (HTTP Live Streaming which Apple uses instead of MPEG-DASH) and FairPlay for encryption	Designed for streaming and sharing media. Not offered as an OOTB solution; you can build your own but not offered as a service.	https://developer.apple.com/streaming/fps/	Apple's Fairplay DRM is explicitly linked to streaming audio/video files and is unlikely to support DLA's file sharing needs. This is the key objection. Other objections include the restrictions when in the Apple trade space and potential hardware requirements for DoD and supplier partners.
Box, Inc.	Box	Public cloud file management hosting solution that is highly integrated with commercially available applications such as Slack and MS Teams.	https://www.box.com/overview	Appeared to be public cloud only and did not meet our feature set completely (file type limitations, data access revocation limitations, complete reliance on online platform). Required DLA content to be migrated from DLA to Box's cloud hosting solution.

Table A-2. COTS DRM Software

Vendor	Solution	Description	Link	Exclusion rationale
Dell EMC	Virtustream's xStream Management Platform and IaaS	Cloud hosting solution and IaaS offering from an endpoint hardware supplier. Files are secure at rest and in transit but do not provide the tracking tools of other solutions.	https://www.delltechnologies.com/en-ca/collaterals/unauth/offering-overview-documents/dell-state-and-local-government-solutions-guide.pdf	Does not specifically provide DRM software.
Fasoo	Fasoo EDRM	EDRM solution focusing on the protection of files using a central policy server and the distribution of a local client to govern access to those files. Highly applicable to DLA's unique requirements and environment.	https://en.fasoo.com/products/fasoo-enterprise-drm/	N/A
Intertrust Technologies Corporation	ExpressPlay, Intertrust Platform	Focused on video and multimedia. Geared toward a media industry.	https://www.intertrust.com/	Too focused on media industry and feature set does not check all our boxes (no watermarking, no data access revocation).
Intralinks	Intralinks UNshare	Niche company for the financial sector.	https://www.intralinks.com/products	Does not appear to accommodate CAD files or manufacturing industry perspectives.
Kudelski	Nagravision	Specializes in providing security for streaming paid content, especially live events and movies.	https://insight.nagra.com/	Streaming only. Does not provide a DRM solution for non-media content.
Locklizard	Locklizard Safeguard PDF DRM Security, Enterprise PDF Security (for Enterprise PDF DRM), Safeguard Secure PDF Viewer	Specializes in PDF copy protection software.	https://www.locklizard.com/digital_rights_management_products/	Limited file types, specifically focused on PDFs.
Microsoft Corporation	Microsoft PlayReady	Must integrate into their app store environment. "Play fair" is not a service. Not offered as an OOTB solution; you can build your own, but not offered as a service.	https://www.microsoft.com/playready/overview/	Would require a custom implementation, which is beyond the scope of our project. In addition, the software is focused on audio and video copy protection.

Table A-2. COTS DRM Software

Vendor	Solution	Description	Link	Exclusion rationale
NextLabs	SkyDRM	EDRM solution focusing on the protection of files using a central policy server and the combination of a web based view only model, as well as the distribution of a local client to govern access to those files.	https://www.skydrm.com/#/home	Required a very large cost in both consulting and licensing fees to facilitate a prototype for DLA. The cost far exceeded what the project could afford.
OpenText	OpenText Media Management	DAM software primarily created to help teams and companies organize their digital media for quick location and retrieval. Specializes in searches through the use of metadata tags.	https://www.opentext.com/products-and-solutions/products/customer-experience-management/digital-asset-management/opentext-media-management	Focus is not on protecting digital data. Some limitations in integrating with existing DLA systems and processes. Feature set was not complete (no location tracking, no watermarking). A custom-built solution would be required.
Oracle	Oracle IRM	Database only. Not offered as an OOTB solution. You can build your own, but not offered as a service.	https://docs.oracle.com/cd/E23943_01/doc.1111/e10724/c05_rights.htm#UCMOV166	Requires installation of Oracle IRM Desktop Client, which communicates back with Oracle IRM Server. Information on the platform was sparse with most documentation being years old. Seems that Oracle IRM is dependent on Oracle Fusion Middleware, Oracles Cloud Platform. These issues of platform adoption requirements in combination with a very limited feature set for DLA's needs compared to other DRM solutions is why it was eliminated.
Pimcore	Pimcore Platform	Specializes in data organization. DAM software primarily created to help companies organize their digital assets.	https://pimcore.com/en/platform	Significant limitations in integrating with existing DLA systems and processes. Feature set was not complete (limited location tracking and automation capabilities).
Seclore Technologies	Seclore Data-Centric Security Platform	Requires data to be moved onto their platform before DRM protections can be applied. Each data file is encrypted security embedded with their document. Focused on the CMMC business.	https://www.seclore.com/digital-rights-management/	Required a very large cost in both consulting and licensing fees to facilitate a prototype for DLA. The cost far exceeded what the project could afford.

Table A-2. COTS DRM Software

Vendor	Solution	Description	Link	Exclusion rationale
Eurostep	ShareAspace	Primarily a document management system geared toward file configuration management.	https://www.eurostep.com/shareaspace-features/	Based on the vendor's marketing documentation, the system's encryption began and ended with logging into their system. DRM is not implemented on the receiving device.
SIMBA	SIMBA Chain	Specializes in Blockchain Technology. Appears to focus on providing an API platform that makes developing software that utilizes blockchain(s) easier.	https://simbachain.com/platform/	The vendor does not provide a DRM solution.
Vaultize Technologies	Vaultize	Provides a DRM COTS Software-as-a-Service solution.	http://www.vaultize.com/index.html	Communication with the vendor proved difficult. After several missed meetings and slow replies to emails the team decided to eliminate the company from the list of prototype candidates.
HelpSystems	Vera	COTS DRM software	https://www.vera.com/product/	The technology's feature set did not meet some of the basic criteria (e.g., no location tracking, no version control, possible issues with automation).
Verimatrix	Verimatrix Video Content Authority System	DRM solution geared toward the protection of streaming video media.	https://www.verimatrix.com/products/vcas/	Video-focused service. File types are limited to media. Content must be stored on the vendor's platform.
Vitrium Systems	Vitrium	COTS DRM software	https://www.vitrium.com/solutions/enterprise-drm	Feature set does not meet some of the basic criteria—userbase size limitation, file type limitations, limited location tracking.

As shown in the table, the most promising vendors appeared to be Fasoo, NextLabs, Seclore, SIMBA Chain, and Vaultize. We then contacted each of the five vendors to obtain more information about their product. Other than SIMBA Chain, all these five vendors provided us with demonstrations of their software.

Browser-Only EDRM Solutions

Although browser-only EDRM solutions were not suitable for this project, they have a number of general advantages, including:

- Installation of a local client is not necessary.
- All access is governed through the web browser.

- The files themselves remain in their original storage location and are not downloaded to client devices.
- Limited changes to the file are possible, such as text edits (EDRM software dependent, and may involve browser plug ins).
- Files can be marked with comments and suggestions (EDRM software dependent and may involve browser plug ins).
- Watermarks can be applied and provide information as to who screen captured or took pictures of the online display.
- To access a file via the browser, the user must log in, allowing the system to track any actions performed against the file.
- The file cannot be forwarded to unknown parties.
- The file is stored on the server, making revocation a straightforward process. The file can be revoked from one or more or all users immediately or a date can be set to determine when the file should no longer be available to one or more users.
- File destruction can be assured since the file is stored on a server that the organization has full control over.
- Disadvantages associated with browser-only EDRM solutions include:
- File functionality is limited to what the browser can support. For example, CAD files cannot be loaded into CAD software for viewing and modification.
- Not all file types can be accessed through a web browser.
- Files cannot be viewed offline or processed/analyzed offline.
- Inability to connect to a supplier's in-house suite of estimation tools.
- Could act like a mandate to use a specific brand of CAD software.

Appendix B

Commercial Best Practices

This section provides an overview of available EDRM tools, techniques, and procedures that are common within the commercial media industry. Specifically, the subsequent research on EDRM best practices is centered on the following questions:

- What have the known EDRM providers and users learned about the deployment of EDRM technology?
- How are companies deploying EDRM technology?

Below are the key findings on commercial best practice for implementing EDRM.

1. Establish Core EDRM Management Practices and Policies

a. Determine Oversight and Governance Structures

It is essential to have an EDRM governance structure in place.¹ One source suggests having a “data owner” or “third party expert” oversee EDRM implementation.²

b. Establish Clear Roles and Responsibilities

Determine who the technology is intended for: Specific individuals? Specific teams or offices?³

c. Build a Content Selection Framework

Determine which content requires EDRM; do not apply this technology indiscriminately.^{4,5}

d. Plan for Scale

Consider how protected content will be used across different platforms/devices and design the solution accordingly: “the less functional the display environment, the less EDRM is required to control that environment.”⁶

e. Develop an EDRM Rollout Plan

Phase EDRM implementation; make use of pilots and proof of concept studies and carefully select use cases.⁷

¹ <https://www2.deloitte.com/ch/en/pages/risk/articles/enterprise-digital-rights-management.html>.

² <https://www.toolbox.com/it-security/identity-access-management/articles/what-is-digital-rights-management/>.

³ <https://www.forgov.qld.gov.au/use-digital-rights-management-and-encryption-for-records>.

⁴ <https://www.toolbox.com/it-security/identity-access-management/articles/what-is-digital-rights-management/>.

⁵ <https://www.forgov.qld.gov.au/use-digital-rights-management-and-encryption-for-records>.

⁶ <https://www.fileopen.com/blog/bid/55094/digital-rights-management-do-s-and-don-ts>.

⁷ <https://www2.deloitte.com/ch/en/pages/risk/articles/enterprise-digital-rights-management.html>.

f. Define and Manage Security Protocols

Example: “Maintain formal encryption/decryption key or password management regimes.”⁸

2. Factor In EDRM End-Users

a. Obtain End-User Buy-In

Examples: Survey prospective end users, conduct a focus group, develop an EDRM blueprint, and send out for end-user feedback.⁹

b. Ensure End-User Experience is Seamless and Convenient

A seamless EDRM experience will ensure end-users use EDRM technology correctly and routinely.¹⁰

c. Leverage Multi-EDRM Solutions to Support Maximize Platform Compatibility (Video)

“A multi-DRM solution basically has license management features for multiple DRMs such as PlayReady, Widevine and FairPlay to support major web browsers and mobile OS.”¹¹

3. Train End-Users on EDRM

EDRM end-users and oversight personnel will require training on how to properly install and use EDRM technology. This will further facilitate buy-in.¹²

4. Layer Technology

“DRM works best when used along with associated solutions like data loss prevention, digital asset management, and content management systems.”¹³

5. Ensure Encryption Schemes Are Multi-Device Compatible

Encryption is a key facet of EDRM.¹⁴ Companies like Verizon appear to select and apply their encryption techniques to promote compatibility across devices for their streaming content.¹⁵

⁸ <https://www.forgov.qld.gov.au/use-digital-rights-management-and-encryption-for-records>.

⁹ <https://www.toolbox.com/it-security/identity-access-management/articles/what-is-digital-rights-management/>.

¹⁰ <https://www.toolbox.com/it-security/identity-access-management/articles/what-is-digital-rights-management/>.

¹¹ <https://pallycon.com/blog/5-things-you-need-to-know-about-multi-drm-technology-part-1/>.

¹² <https://www.naa.gov.au/sites/default/files/2019-09/IM-Standard-Implementing%20an%20EDRMS%20key%20considerations-V1.0%202011.pdf>, page 21–22.

¹³ <https://www.toolbox.com/it-security/identity-access-management/articles/what-is-digital-rights-management/>.

¹⁴ <https://www.vitrium.com/blog/hassle-free-drm>.

¹⁵ <https://www.verizondigitalmedia.com/blog/best-practices-for-deploying-drm-in-a-large-scale-ott-stack/>.

Appendix C

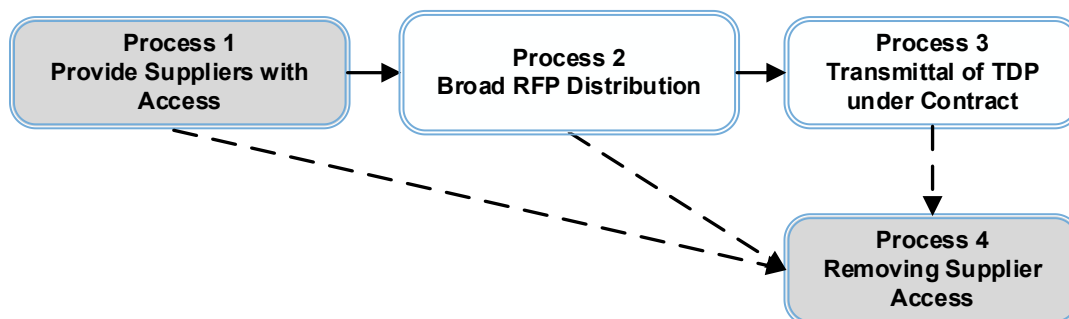
EDRM Implementation Process Flows

EDRM implementation can significantly increase the security level of TDP during the procurement process. There are two main areas, listed below, where EDRM can have an immediate impact to increase security.

- DLA's broad distribution of RFPs to prospective suppliers, which provide bid packages containing TDP.
- The back-and-forth transmittal of TDP with contracted suppliers at any point during the production of parts and products.

Figure C-1 provides a high-level view of the processes involved in the augmentation of the procurement process with EDRM.

Figure C-1. High-Level View of Processes

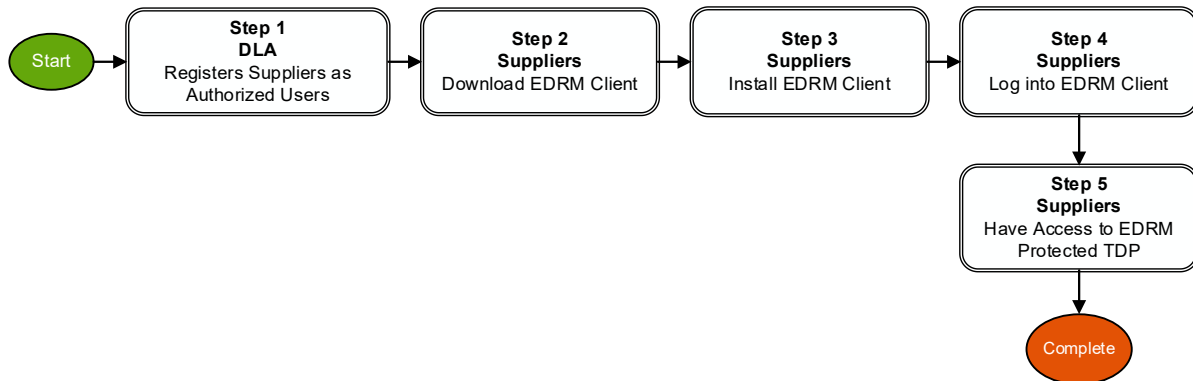


- Process 1 allows DLA to provide suppliers with access to the EDRM protected TDP.
- Process 2 details how TDP is protected during the initial RFPs.
- Process 3 illustrates where EDRM can protect TDP during the execution of the procurement contract.
- Process 4 involves DLA removing EDRM access from those suppliers who no longer have a need for accessing protected TDP.

Processes 1 and 4 are new and allow DLA to add and remove a supplier's access to EDRM protected TDP. Processes 2 and 3 are currently part of procurement and detail where EDRM would augment those two processes.

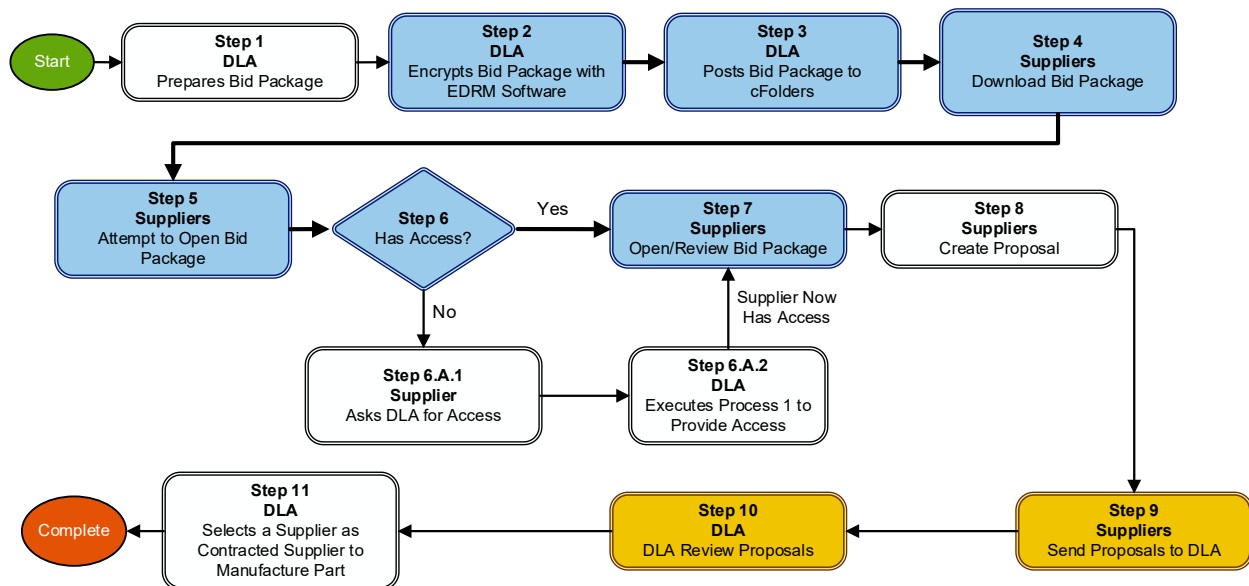
Process 1—Providing Suppliers with Access

For suppliers to access EDRM protected data, they must be registered with the EDRM policy server as an authorized user. Suppliers can then download and install the local client to gain access to the protected TDP.

Figure C-2. Process 1: Providing Suppliers with Access

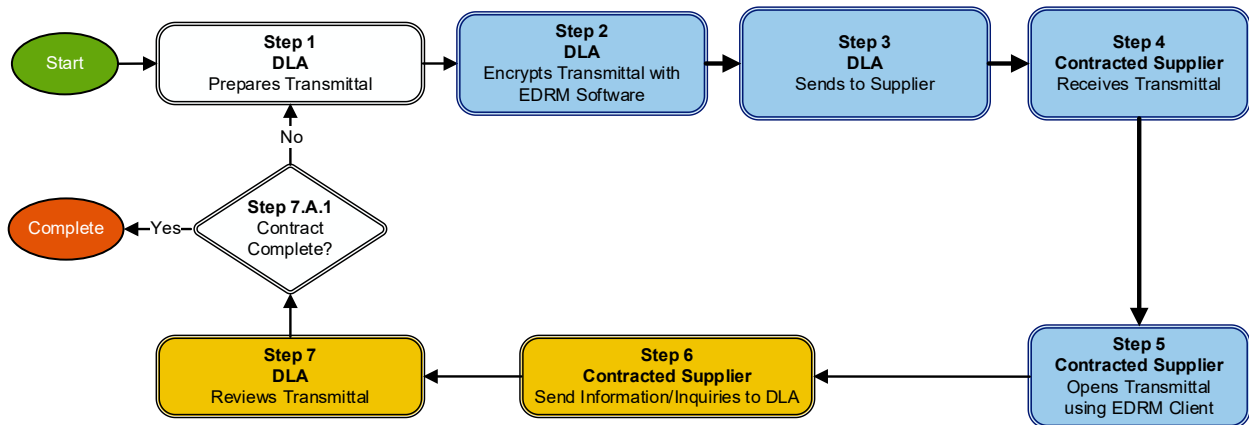
Process 2—Broad RFP Distribution

TDP included with RFPs can be protected with EDRM. Figure C-3 indicates in green where data can be protected with EDRM. The yellow borders identify the steps where the supplier may choose to use EDRM to protect data sent to DLA

Figure C-3. Process 2: Broad RFP Distribution

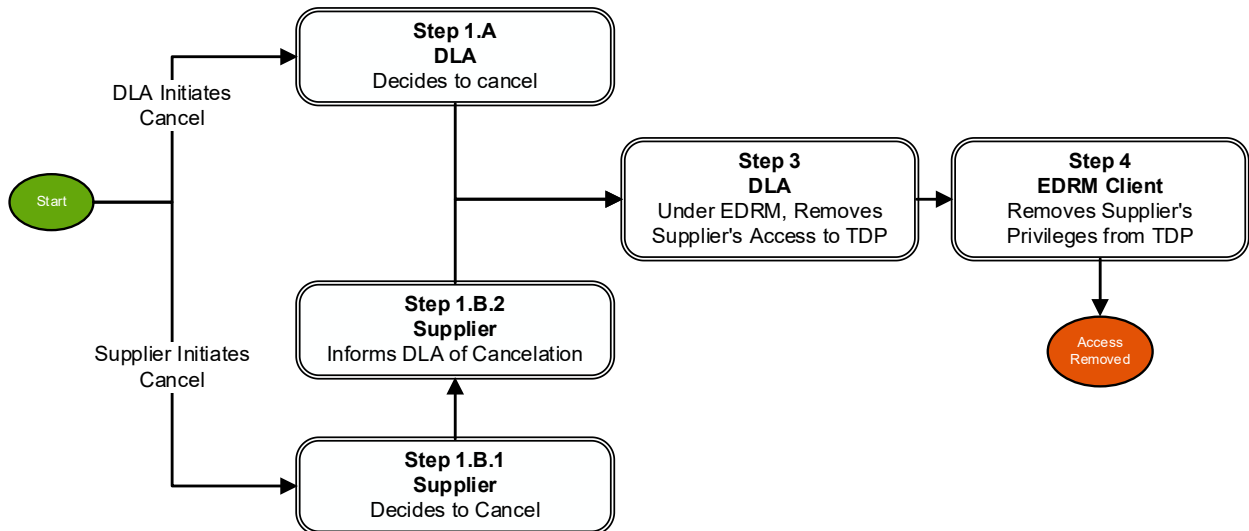
Process 3—Transmittal of TDP under Contract

Figure C-4 illustrates the back-and-forth conversations between DLA and the Supplier at any point during the production of the product. The steps in green indicate where the TDP would be protected with EDRM, while yellow designates the steps where suppliers may choose to use EDRM to protect the data sent back to DLA.

Figure C-4. Process 3: Transmittal of TDP Under Contract

Process 4—Remove Supplier Access

At any point during the previous three processes, DLA can remove a supplier's access to EDRM protected TDP. Figure C-5 illustrates this point and shows how a supplier can initiate the cancellation of rights themselves.

Figure C-5. Process 4: Remove Supplier Access

Appendix D

Functional Requirements

From our initial 17 high-level evaluation criteria, LMI derived more detailed requirements, totaling 51 for purposes of our vendor software selection (Table D-1).

Table D-1. Functional DRM Requirements for DLA

Requirement identification	Description	Rating
R0.1	The prototype leverages commercially available products, or components thereof, that require little-to-no tailoring to demonstrate solutions.	
R0.2	Potential solutions study information encryption, management of permissions, offline access, data at rest, and auditing.	
R0.3	Prototypes unlikely to result in a viable pilot project are not considered.	N/A
R0.4	Each candidate prototype contains, in addition to prototype description, an approximated cost, time to delivery, level of effort, and likelihood of viability.	
R1	DLA has the capability to advertise the procurement bid package.	
R2.1	DLA can transfer data to many users securely, with data protected by EDM.	
R2.2	DLA-transferred data has validity checks.	
R2.3	DLA-transferred data must arrive intact.	
R2.4	Data must remain intact once it arrives.	
R3.1	EDRM protection offers security in transit, thwarting interception (data in transit).	
R3.2	DLA can apply access permissions to the data.	
R3.3	DLA can apply unique access permissions by user.	
R4.1	DLA can track any alterations of data protected by EDM.	
R4.2	DLA can track modifications (i.e., what changed).	
R4.3	DLA can determine who made the change.	
R4.4	DLA can determine when the change was made.	
R4.5	DLA can determine where the change was made.	
R4.6	DLA can determine the seriousness of the change.	

Table D-1. Functional DRM Requirements for DLA

Requirement identification	Description	Rating
R4.7	DLA can furnish this information (R4.3–R4.6) for forensics investigation.	
R5.1	DLA has control of data distribution (who can get the data).	
R5.2	DLA can ensure that the data has been destroyed.	
R5.3	DLA can deny access to requestors.	
R6.1	DLA can track who requests protected data.	
R6.2	DLA can track who receives protected data (who got the data).	
R6.3	DLA can track who transfers protected data.	
R6.4	DLA can exercise data access revocation.	
R6.5	DLA can exercise data access expiration.	
R7.1	Suppliers are prevented from redistributing data without permission from DLA.	
R7.2	DLA is notified of attempts to redistribute data.	
R8	DLA can grant permission to a supplier to redistribute data (with data remaining under DLA control).	
R9.1	Supplier can transfer data to DLA securely, with data protected by EDRM.	
R9.2	Supplier-transferred data has validity checks.	
R9.3	Supplier-transferred data must arrive intact.	
R10	DLA can obtain identity checks on sources of data transferred to DLA.	
R11	Supplier can send data securely for change requests, with their data protected by EDRM (data sent from the Supplier to DLA, indicating to change in the TDP, e.g., engineering change request).	
R12	DLA can approve change requests.	
R13	The EDRM solution cannot hinder any typical external interface or the functionality expected by DLA partners and suppliers (e.g., “any typical” refers to processes, such as suppliers consuming the TDP from DLA as they do now, allowing them to verify CAD drawings using software tools and create derivative products, like computer numerical control machine tool programming products).	
R14	The EDRM solution has a high enough level of maturity (technology readiness level) to be elevated to a pilot project with a high potential to move into production.	

Table D-1. Functional DRM Requirements for DLA

Requirement identification	Description	Rating
R15	The EDRM solution considers the practicality of preventing unauthorized disclosure through screenshots and selective copying of portions of a document.	
R16.1	The platform facilitates the sharing and security of relevant file types.	
R16.2	The platform facilitates the sharing and security of relevant sizes.	
R17	Scaling up the platform to meet DLAs needs does not pose a significant challenge (for example, DLA publishes tens of thousands of items each month for procurement processing for the over 200,000 manufacturing firms in the U.S.).	
R18	The platform can pair easily with DLA's enterprise systems (i.e., DIBBS).	
R19	The platform does not affect DLA processes and operations significantly. (The as-is documentation describes the relevant processes.)	
R20	The platform integrates with DLA's data repositories, acting only as conduit.	
R21	The platform presents only minor changes to DLA users' workflow.	
R22	The platform tracks user activities and behavior patterns for analytics.	
R23	The platform offers a feature to watermark data.	
R24	The platform presents only minor change to systems and workflows of DLA partners.	
R25	The platform can track the location of DLA data and user access.	
R26	The platform enables DLA to automate low-level processes (to be identified) with minimal support from staff (e.g., automate setting the expiration date for a week after the bids are due).	

Note: N/A = not applicable.

Appendix E

Test Plan

After identifying requirements our prototypes must meet to secure TDPs, we developed a plan for testing their ability to meet those requirements. We called this the Test Plan. It was submitted to DLA in August 2021.

As discussed in Chapter 3, the Test Plan is organized around six tasks, each containing various test case sets, corresponding actions, and sub-tasks that serve as evaluation metrics to help our SMEs evaluate the suitability of EDRM for DLA. There are a total of 176 sub-tasks and tasks in the Test Plan, and our testers systematically evaluated the ability of the prototype to achieve each one.

Each of the test case sets map to our 51 requirements and expand on each requirement by testing the requirement from several angles, highlighting any limitations and advantages when considering EDRM in DLA's environment.

An updated version of the Test Plan that we provided in August 2021 follows, with modifications to account for the expanded data set used to evaluate the DRM software.

DIGITAL RIGHTS MANAGEMENT TO SECURE TECHNICAL DATA PACKAGES

TEST PLAN

VERSION 1.3

VERSION DATE: 8/23/2022



7940 JONES BRANCH DRIVE
TYSONS, VA 22102

Revision History

Date	Version	Description	Author
3/26/2021	1.0	Initial document created.	Chuck Lorence
5/11/2021	1.1	Updated to reflect changes in the test cases document.	Chuck Lorence
6/10/2021	1.2	Updated after peer review feedback.	Chuck Lorence
7/13/2021	1.2.1	Comments.	Ben Kassel
8/17/2021	1.3	Updated to address feedback. Added appendix.	Shannon Marnien Martin Shinko Chuck Lorence
8/23/2022	1.3.1	Updated to be more inclusive of prototyping methodology.	Matt Bishof

Contents

1. Introduction	1
1.1 Purpose	1
1.2 Background	1
1.3 Test Items.....	1
1.4 Scope	2
1.4.1 Features Tested	2
1.4.2 Features Not Tested.....	2
1.5 Assumptions, Constraints, and Risks	3
1.5.1 Assumptions.....	3
1.5.2 Constraints	3
1.5.3 Risks and Contingencies	3
2. Test Strategy	4
2.1 Test Levels	4
2.2 Types of Testing	4
3. Tools	4
4. Test Environment	5
5. Resources	5
5.1 TDP for Testing	5
5.2 Staffing	6
5.3 Training Needs	6
6. Test Results	7
Appendix A. Test Cases	8
Scope	8
Layout.....	8
Normal Operational Sequence Represented by Tasks.....	9
A.1 Testing References	9
A.1.1 Requirements	9
A.1.2 TDP Contents (Also Known as Test Data).....	10
A.1.3 Terminology and Definitions	10
A.1.4 Global Test Case Assumptions.....	10
A.1.5 DLA Methods of Furnishing TDP	10
A.1.6 OEM Methods of Sending the TDP Back to DLA.....	11

A.1.7	DRM Policies	11
A.1.8	DRM Policy Sets.....	11
A.1.9	Ways to Request Permissions	12
A.1.10	Evaluation Expectations	12
A.2	Task 1: Transfer Data to Many Users Securely	12
A.2.1	Purpose	12
A.2.2	Requirements	13
A.2.3	Assumptions	13
A.2.4	Test Case Set 1.1: Verify DRM Policies Function as Described... 13	
A.2.4.1	Permutations.....	13
A.2.5	Test Case Set 1.2: Evaluate Advertisement Options.....	15
A.2.5.1	Permutations.....	15
A.2.6	Test Case Set 1.3: Transfer Data to Many Users Securely	16
A.2.6.1	Permutations.....	16
A.2.7	Test Case Set 1.4: Assign Access Permissions to DLA and Non-DLA Users.....	17
A.2.7.1	Permutations.....	17
A.2.8	Test Case Set 1.5: Policy Automation	18
A.2.8.1	Permutations.....	19
A.3	Task 2: Transfer Data Securely in Reverse	19
A.3.1	Purpose	19
A.3.2	Requirements	19
A.3.3	Assumptions	19
A.3.4	Test Case Set 2.1: Transfer Data Securely in Reverse	20
A.3.4.1	Permutations.....	20
A.3.5	Test Case Set 2.2: Transfer Data Generated by the OEM in Its Enterprise Securely in Reverse.....	21
A.3.5.1	Permutations.....	21
A.4	Task 3: Transfer Data Securely with Validity Checks	22
A.4.1	Purpose	22
A.4.2	Requirements	22
A.4.3	Assumptions	22
A.4.4	Test Case Set 3.1: Check the Validity of Data Transferred from DLA to the OEM	22
A.4.4.1	Permutations.....	23

A.5	Task 4: Transfer Data Securely in Reverse with Validity Checks	23
A.5.1	Purpose	23
A.5.2	Requirement	24
A.5.3	Assumptions	24
A.5.4	Test Case Set 4.1: Check Validity in Reverse	24
A.5.4.1	Permutations	25
A.6	Task 5: Collect Forensic Information and Check the Identity of the Recipient.....	26
A.6.1	Purpose	26
A.6.2	Requirements	26
A.6.3	Assumptions	26
A.6.4	Test Case Set 5.1: Control Access to the TDP	26
A.6.4.1	Permutations.....	27
A.6.5	Test Case Set 5.2: Local Agent—Identify Who, When, and Where	27
A.6.5.1	Permutations.....	27
A.6.6	Test Case Set 5.3: Browser—Identify Who, When, and Where....	29
A.6.6.1	Permutations.....	29
A.6.7	Test Case Set 5.4: Access a Copy of the TDP	30
A.6.7.1	Permutations.....	30
A.6.8	Test Case Set 5.5: Supply Information about Changes	30
A.6.8.1	Permutations.....	31
A.6.9	Test Case Set 5.6: Check Identity and Validity Concurrently.....	31
A.6.9.1	Permutations.....	31
A.6.10	Test Case Set 5.7: Report on User Behavior.....	32
A.6.10.1	Permutations	32
A.6.11	Test Case Set 5.8: Support Investigation	32
A.6.11.1	Permutations	32
A.7	Task 6: DRM Software Information.....	33
A.7.1	Purpose	33
A.7.2	Requirements	33
A.7.3	Assumptions	33

A.7.4 Test Case Set 6.1: Integration	33
A.7.4.1 Permutations.....	33

Tables

Table 1-1. Features Tested.....	2
Table 1-2. Features Not Tested	3
Table 2-1. Types of Testing	4
Table 4-1. EC2 Software Configuration	5
Table 5-1. TDP Files	5
Table 5-2. Test Roles and Responsibilities.....	6
Table 5-3. Training Needs	6

1. Introduction

The Defense Logistics Agency (DLA) Digital Rights Management (DRM) to Secure Technical Data Packages (TDPs) Project (hereafter referred to as the DLA-DRM Project) explores the ability of commercial DRM products and techniques to improve the security of the TDPs that DLA is required to furnish to its potential suppliers in support of competitive procurements. During this project, one or more prototypes are being developed to validate the benefits of different techniques and support informed comparisons between potential options for securing technical data. This test plan focuses on the test and evaluation of the prototypes.

1.1 Purpose

This test plan describes the evaluation of prototypes for their ability to improve the security of TDPs. This plan addresses those items and elements related to the testing process only, including directly and indirectly affected elements. The test plan primarily focuses on ensuring that the project evaluates DRM technologies in accordance with the requirements.

1.2 Background

The technologies prototyped as part of the DLA-DRM Project are commercial-off-the-shelf (COTS) solutions. Our testing targets involve the following aspects of these COTS systems:

- Examining the application of protective permissions and encryption to TDP
- Verifying the application of security policies to TDP
- Exploring the capabilities and limitations of various TDP delivery methods using DRM
- Discovering the estimated level of effort required to integrate protective techniques into DLA's business processes.

1.3 Test Items

The DLA-DRM Project uses the Jira project management software package to manage and track the progress of individual sprint's development and testing. Tickets¹ for a particular sprint are added to Jira and assigned to the team in a Sprint Planning meeting. Tickets executed for a particular sprint come from decisions during the Sprint Planning meetings.

This project splits the test items into two categories (three if custom development is required). The first category includes the Jira tickets designated for a particular sprint specific to that software development lifecycle (SDLC) iteration. The second category consists of test cases created to evaluate and verify DRM functionality based on the requirements and scenarios of DLA's processes, environment, and expectations for DRM technology. Appendix A contains the test cases document.

¹ A ticket defines a task and the acceptance criteria for evaluating correct completion of the task.

In addition to the sprint requirements, testing of the following occurs if any custom development is required:

- System functionality affected by the ticket requirements and code changes
- Any reports that may be affected by the build changes
- User access to the changes included in the ticket or release
- System regression testing before release, if applicable given the sandbox or research nature of this project.

1.4 Scope

The scope of testing involves those tickets assigned to the active sprint's backlog. The tester uses the ticket requirements and acceptance criteria to evaluate the testing scope. Testers use the ticket's acceptance criteria to test the implementation of the requirements. Testing occurs during a sprint or iteration for each ticket; using Jira, testers report, track, and facilitate the resolution of problems encountered during testing. Testers may not test functionality not affected by sprint tickets.

Testing for the DLA-DRM Project is limited to functional testing only. The following sections describe features tested or not tested.

1.4.1 Features Tested

The following features are tested using an exhaustive list of functional test cases. Specific features tested are selected in increments and include the tickets selected for a sprint.

Table 1-1. Features Tested

Feature	Software	Criticality to Deployment Success	Testing Priority	Notes
COTS	Fasoo	High	High	Primary prototype to evaluate DRM implementation.
Custom	Use of Blockchain	Low	Medium	DRM solution with blockchain technology.
COTS	NextLabs	Low	Low	A backup if the team is unable to use the primary COTS software.

1.4.2 Features Not Tested

The following features are not requirements for the DLA-DRM Project and are not tested.

Table 1-2. Features Not Tested

Feature	Software	Criticality to Deployment Success	Testing Priority	Notes
Performance	All COTS	N/A	N/A	Testing of performance requires time, tools, and methods beyond the scope of the project.
Bugs and Fixes	All COTS	N/A	N/A	Any bugs discovered during the evaluation of COTS software are noted for the vendor to resolve.

1.5 Assumptions, Constraints, and Risks

This section describes the assumptions, constraints, and risks associated with performing the DLA-DRM Project.

1.5.1 Assumptions

The study team assumes that little, if any, software development will occur during this project. Therefore, all testing is geared toward verification or evaluation of the functionality of the COTS software.

1.5.2 Constraints

The software evaluated is COTS software. Therefore, individual testing is limited to what the software allows.

1.5.3 Risks and Contingencies

The team has uncovered several risks associated with carrying out the project as expected as well as strategies to mitigate them:

- The COTS software vendor may not add functionality without additional payment beyond our other direct costs budget. If this occurs, we may need to abandon our evaluation of that vendor's product and switch to another.
- One or more of the COTS software may not offer the functionality we plan to evaluate. If this occurs, we will verify the non-existence of the functionality with the vendor. If the functionality does not exist, we note the absence in the results of the test case.
- Unanticipated interactions with other software and potential security vulnerabilities could occur when installing the COTS software. To reduce this risk, we run the software in a standalone Amazon Web Services (AWS) testing environment.
- Microsoft Windows file-handling practices, which add metadata to files as they are handled (but not edited) within the operating system (OS), may disrupt independent validity checks of the TDP. If this proves true, the team documents the finding as a shortcoming of the DRM implementation and explains its cause.

2. Test Strategy

Given the verification and evaluation nature of the DLA-DRM Project, the test strategy characterizes the COTS software's ability to satisfy metrics in the test cases. Testing ends for the COTS software when all test cases have been completed.

2.1 Test Levels

Testing for the DLA-DRM Project is limited to functional testing only. The COTS test environment consists of an AWS private cloud running several AWS Elastic Compute Clouds (EC2s). The team uses the EC2s to test COTS software via a software-as-a-service architecture. Section 4 contains additional information about the test environment.

2.2 Types of Testing

Table 2-1 shows the typical types of testing.

Table 2-1. Types of Testing

Test Type	Description
Peer Review	Peer reviews are performed and tracked in Jira.
Functional	Functional testing is a quality assurance process and type of black-box testing that bases test cases on specifications of the software component under test. Functions are tested by feeding them input and examining the output. Functional testing evaluates the compliance of a system or component with specified functional requirements. The DLA-DRM Project relies heavily on functional testing using test cases to evaluate how DRM is implemented by DRM software.
System	System testing typically involves testing the system as a whole with the goal of proving the system functionality and performance, as designed. This project's testing is more narrow in focus, concentrating on the evaluation of DRM capabilities and how they contribute to the protection of TDPs used by DLA for the acquisition of manufactured parts and not the overall functionality of the COTS software itself. Therefore, system testing is not performed.
Security	• Evaluating the ability of COTS software to prevent unauthorized access to the TDP. • Evaluating data protection in transit: testing for man-in-the-middle attacks, and validating that the TDP has not been altered in transit. • Evaluating data protection for data at rest: evaluating the software's ability to ensure files are accessible to those with the proper permissions only. • Evaluating data protection for data in use: evaluating the software's ability to limit what authorized and unauthorized users can and cannot do while accessing the technical data in the TDP.

3. Tools

The DLA-DRM Project uses the following recommended LMI SDLC tools:

- Atlassian Jira for requirements and test tracking
- Confluence for documentation
- SharePoint for documentation.

4. Test Environment

The DLA-DRM Project test environment resides in the project's AWS cloud and consists of several AWS EC2s running Windows Server 2016 operating system (see Table 4-1).

Table 4-1. EC2 Software Configuration

Type	Name
Operating System	Windows Server 2016
Browser	Google Chrome
Browser	Microsoft Edge
Office Suite	Microsoft Office 2016 • Word • Excel • PowerPoint • Outlook
Computer-aided design (CAD)	Fusion 360 7.0
PDF Viewer	Adobe Reader DC 2021
Compression	7-Zip 12.02
Network Protocol Analyzer	Wireshark 3.4.7

5. Resources

This section describes the resources needed to perform testing for the project.

5.1 TDP for Testing

The DLA-DRM Project focuses on protection and transmission of TDP data. This section describes the data used during the test and evaluation of the prototypes.

PDF and Zip files transport the TDP contents as a complete package from point A to point B. The DLA-DRM Project uses a PDF file with embedded CAD data and CAD files attached. When warranted by the test case or task, the project combines all the files into a single Zip file.

Table 5-1 shows the files in the TDP for testing.

Table 5-1. TDP Files

File Name	Native Application	Description
DRM001.pdf	Adobe three-dimensional (3D) PDF	TDP containing attached STEP ^a file, simulating the TDP distributed to prospective bidders.
DRM002.pdf	Adobe 3D PDF	TDP containing three attachments, simulating a TDP with an as-designed view of the product for review prior to approval for manufacture (or to represent as-built data delivered with the product).
Solicitation.pdf	Adobe PDF	An ordinary two-dimensional PDF file; this is an abbreviated portion of a request for procurement.

File Name	Native Application	Description
Link_Assembly_Bill_Of_Material.xlsx	Microsoft Excel	Spreadsheet containing the engineering bill of material for the entire coupling link assembly (part # 11-1-1717 is the information for the side link).
Air_Drop_Platform_Rigging_manual.docx	Microsoft Word	Pages taken from a field manual for rigging airdrop platforms to make a file in Word format (converted from a PDF file).
Sample_Acceptable_3D_TDP.pptx	Microsoft PowerPoint	Example PowerPoint presentation containing one slide about acceptable 3D formats.
linkSidePlate_DRM01_2.STEP	(Text file) common CAD data exchange format	(Attachment file in DRM001) STEP file corresponding to the CAD data in file DRM001.pdf.
linkSidePlate_DRM01_1.stl	(Text file) common CAD data exchange format	(Attachment file in DRM002) STL file derived from a CAD file, simulating manufacturing data.
couplingSideLink.f3d	Autodesk Fusion 360 CAD software	(Attachment file in DRM002) Fusion 360 native CAD file used to make file DRM002.pdf.

^a STEP—Standard for the Exchange of Product data. A STEP-File contains model data in clear text format that is recognized by many computer-assisted design (CAD) software platforms.

5.2 Staffing

Table 5-2 shows the staffing assumptions for the project.

Table 5-2. Test Roles and Responsibilities

Full-Time Equivalent	Role, Organization	Specific Responsibilities/Comments
5	Test engineers, LMI	Responsibilities: • Execute tests • Log results and findings • Recover from errors

5.3 Training Needs

The testing training needs for the DLA-DRM Project consist of understanding the COTS software tested. Table 5-3 shows the training needed.

Table 5-3. Training Needs

Name of Resource	Skills Needed	Plan
Fasoo DRM software	Working knowledge of the system.	Team members attend a Fasoo-furnished training session and review the software user guides.
Blockchain	Working understanding of blockchain technology.	Team members attend presentations by LMI blockchain subject matter experts (SMEs) to become familiar with the technology. In addition, two or more team members research the technology applicability to DRM.
Overview of Fusion 360 CAD software	Background knowledge of output products.	Team members attended a demonstration of use of the software to create a CAD file.

6. Test Results

The results of any tests performed against a Jira ticket are captured in that Jira ticket. For the test cases, test results are captured in the test case document assigned to a particular COTS software.

Given the verification and evaluation nature of this project, test results are evaluated as a whole and discussed as a team to develop findings for the final report.

Appendix A. Test Cases

This appendix contains the test cases used to explore and validate the benefits of different techniques utilized by COTS DRM software vendors and make informed comparisons between potential options for securing technical data.

Scope

Each test case is scoped to evaluate a particular aspect of DRM technology or technology to augment DRM technology. Given the exploratory nature of the project, the test cases are written as guidelines for the testers, allowing them the freedom to explore the COTS software's capabilities without the restriction of a particular outcome. As such, the test cases do not follow the typical software engineering practice of providing a test, expected outcome, and an indication of pass or fail. Instead, these test cases set parameters for exploration and require testers to record their findings as a detailed explanation.

DRM controls are not expected to be applied in DLA. Data used by DLA personnel is held in the Department of Defense (DoD) secure perimeter firewall and government data rights—even the Limited Rights Notice in the *Federal Acquisition Regulation* (FAR) (as of October 2018)—permit sharing data within the government (i.e., as specified in FAR sect. 52.227-14, page 52.2-283, “These data may be reproduced and used by the Government with the express limitation that they will not ... be used for purposes of manufacture nor disclosed outside the Government”). Restrictions are not applied to data access among and between groups of DLA employees. Therefore, the evaluation of prototypes is limited to communication between the DLA and organizations outside of the DLA network. The scope of the evaluation does not include interactions between DLA personnel in their own network.

Layout

Testing is divided into several distinct tasks. Each task includes the following information:

1. Purpose, with a high-level overview of the DRM functionality evaluated in the test cases
2. Requirements, listing the requirements (referenced from the *Digital Rights Management to Secure Technical Data Packages Requirements Definition* document) covered by the task
3. Assumptions, including those the tester may take for granted while working through the test cases
4. Test case sets, which define individual sets of test cases grouped beneath a task.

Normal Operational Sequence Represented by Tasks

The test case tasks represent steps in the sequence of the DLA processes for procuring parts or services to support the sustainment phase of weapon systems. The normal operational sequence for a procurement follows:

- **Step A.** DLA advertises the procurement under DRM (by email, posting on a web page, etc.); e.g., in Task 1, Test Case Set 1.2, 3.5.1 Permutations, Listing on a website.
- **Step B.** Technical data, under DRM, can be securely transferred to many users (Task 1); i.e., the transfer of data from DLA to the original equipment manufacturer (OEM).
- **Step C.** Step B with validity checks (Task 3); i.e., DLA verifies that the data the OEM receives was the same data DLA furnished.
- **Step D.** Step B with identity checks (only applies to the transfer of data from DLA to the OEM, as addressed in Task 5); i.e., DLA verifies that the recipient of the data was the intended recipient.
- **Step E.** The OEM securely sends a change request under DRM (covered in Tasks 1 and 2).
- **Step F.** Collect forensic information (Task 5).
- **Step G.** Technical data, under DRM, can be securely transferred in reverse (Task 2).
- **Step H.** Step G with validity checks (Task 4); i.e., DLA verifies the data received was the same data sent by the OEM.
- **Step I.** DLA approves the change (by email or through data can be transferred capability, such as in Task 1). This step does not involve DRM.²

These test case tasks do not represent the entire sequence of steps in the procurement process, such as DLA awards a contract or DLA-authorized payment for goods or services delivered. However, these tasks represent the steps related to technical data. Also, the bid process can be iterative, with additional rounds of technical data transferred between DLA and a manufacturer. Those additional rounds are represented adequately by the set of steps described.

A.1 Testing References

This section defines those items common to all test cases.

A.1.1 Requirements

LMI's *Digital Rights Management to Secure Technical Data Packages Requirements Definition* contains the requirements referenced in this document. Sections 3 and 4 of this test plan describe the testing environment and tools used during testing.

² This step does not necessarily involve DRM, but DLA could use a pathway protected by DRM instead of email. If DLA approval comes from a DRM protected pathway, testing of that method fits under Task 1, so no other DRM methods specific to this step need testing.

A.1.2 TDP Contents (Also Known as Test Data)

Unless otherwise specified, the TDP (and its contents) used for testing consists of the files documented in Section 5.1 of this test plan.

- **DRM permissions.** Each file in the envelope as well as the envelope itself are assigned DRM permissions.
- **Modifications.** OEMs who submit change requests modify one or more of the TDP files and send them back to DLA with or without the original envelope. This method maintains the files' original DRM protections.

A.1.3 Terminology and Definitions

The table defines various terminology in this appendix.

Term	Definition
Accesses	When a user attempts to open a file.
COTS	Commercial off-the-shelf, a commercially available product ready for use without requiring customization.
DRM software	DLA's DRM software. The OEM operates under DLA's license for DRM software and, thus, uses the same DRM software as DLA.
LDAP	Lightweight directory access protocol, for directory services authentication.
Local agent	Software furnished by the DRM software vendor and installed on the user's machine. This software communicates with the DRM central server and implements restrictive policies.
OEM	Original equipment manufacturer, a manufacturer considering bidding on an advertised procurement opportunity.
Procurement	Action of DLA in procuring parts or services to support the sustainment phase of weapon systems.
P-TDP	Procurement TDP, equivalent to TDP.
TDP	Technical data package, contains all the files the OEM needs to understand the procurement opportunity.
Received	When a user obtains a file, even though that user might be unable to open that file.
Reverse transfer	The transfer of data from the OEM to inbound data store of DLA.
Vendor	The vendor of the DRM software, not the OEM considering bidding on a procurement opportunity.

A.1.4 Global Test Case Assumptions

- The tester has access to all the tools needed to execute assigned test cases, including any software to view or modify the files in the TDP.
- Data is a well-formed TDP or another appropriate file format (e.g., plain PDF).
- A collection of authorized users exists representing OEM users and the central DLA authority.
- Security access logs are created based off successful and failed actions.

A.1.5 DLA Methods of Furnishing TDP

The table shows the various methods for furnishing TDP.

Method Name	Description
DLA method 1: Download from website	General Hypertext Markup Language website (C-folders equivalent)
DLA method 2: Email attachment	Microsoft Outlook (or something equivalent)
DLA method 3: Copy from local storage device	N/A; DLA does not furnish data this way

A.1.6 OEM Methods of Sending the TDP Back to DLA

The table shows DLA's ideal methods for receiving TDP from OEMs.

Method Name	Description
OEM Method 1: Upload using a website	Simulated website
OEM Method 2: Email attachment	Microsoft Outlook
OEM Method 3: Copy from local storage device	Thumb drive
OEM Method 4: Secure File Transfer Protocol	AWS Simple Storage Service bucket

A.1.7 DRM Policies

The table shows individual policies in the DRM software. These policies were copied from page 28 of the *Fasoo Admin Guide* but are typical of policies for COTS DRM software.

Policy Name	Definition
Edit	Allows a user to edit and save a document, including copying and pasting contents from a secured document to another secured document, if the user has edit permission to both documents.
View	Allows a user to view a document. The user does not have permission to edit the document but may have permission to save the document under another name with the same DRM restrictions. The user does not have permission for copying and pasting, etc.
Print	Allows a user to print a document.
Screen capture	Allows a user to capture an image of a document using the print screen key or screen capture programs when a secured document is opened.
Change permission	Allows a user to grant additional permissions to other users and change the owner of a document.
Print with watermark	Allows a user to print a document with a watermark.
Extract	Allows a user to copy contents from a secured document and paste them into a plain document or other unsecured locations, such as the body of an email.
Decrypt	Allows a user to decrypt a secured document into a plain document.
Change class	Allows a user to change the document class of a document.
Macro	Allows a user to use macro functions.
External sharing	Allows a user to convert a document for external sharing.

A.1.8 DRM Policy Sets

The table depicts realistic policy sets. These sets are not all the possible policies and policy combinations. Rather, they are the most likely to be used.

Policy Set Name	Policies
Policy Set 1 (Fort Knox)	View only. Must view in a native application (with local agent application active) or the browser only.
Policy Set 2 (Amsterdam)	Allow: view, edit, print with watermark, copy and save as a new file, extract, decrypt, and external sharing.

A.1.9 Ways to Request Permissions

The table shows methods for an OEM to request permission or elevated permissions on a TDP.

Method for Requesting Permissions	Description
Agent installed locally	Use an agent to request a higher permissions level.
Request permission via email	N/A (although DLA could unilaterally revise permissions to allow additional access).
Request through online web application	Use the mechanism built into the prototype's client for requesting permission for higher privileges.
Operate under DLA's license for DRM software and, thus, use the same DRM software as DLA—with the same local agent app	Ideally, no action is required by the OEM to provide DLA access to a TDP coming from an OEM but anomalies may occur.

A.1.10 Evaluation Expectations

During the evaluation process, testers follow these rules:

1. Unless otherwise specified in the test case, testers decide the test data used to execute the test case.
2. Unless otherwise specified, the test data is pulled from the test data prepared for this project (see Section 5.1 of the Test Plan).
3. Each evaluation uses the following format for recording findings in the Evaluation column of the Permutations column. Labels (e.g., test data) are included:
 - a. Test data: Testers indicate the test data used during the evaluation.
 - b. Evaluation: Testers note their evaluation results in narrative format.

A.2 Task 1: Transfer Data to Many Users Securely

A.2.1 Purpose

Task 1 tests the basics of DRM: verifying data can be transferred securely using DRM policies. It includes the following actions:

- Verify DRM policies function as described.
- Evaluate advertisement options using the DRM software.
- Transfer data to many users securely.
- Assign access permissions to groups of non-DLA users.
- Make TDPs available for access by non-DLA users without operating under DRM software or policies (i.e., DLA is in the DoD secure perimeter firewall).
- Create and apply access permissions to files, data stores, and users.

A.2.2 Requirements

R1, R2.1, R2.3, R2.4, R3.1, R3.2, R3.3, R5.2, R5.3, R6.4, R6.5, R7.1, R7.2, R8, R15, R16, R20, R21, R23, R26

R0.2—Offline access, data at rest, permission management, and encryption implemented.

A.2.3 Assumptions

- Unauthorized users could still receive a TDP in our test cases, e.g., as a manual file copy from an authorized source to simulate an unintentional access opportunity.
- The OEM has installed the vendor's local agent (except for browser test cases).
- LDAP is configured with a set of authorized users.

A.2.4 Test Case Set 1.1: Verify DRM Policies Function as Described

Overview:	Evaluate how the policies function in practice. Pay specific attention to the policy definitions and the verification of those definitions. For example, if a policy to prevent editing is applied, then the assumption is zero edits are allowed. In addition, the test cases explore revoking access once it is granted to a user.
Requirements:	R0.2, R3.2, R5.2, R6.4, R6.5, R7.1, R7.2, R8, R15, R16, R20, R23, R26
Preconditions:	1. The TDP package is available as a PDF and Zip file. 2. The TDP does not have any policies applied—i.e., it's a clean slate.
Postconditions:	Each DRM policy from the software has been tested in the local agent and the browser.
Assumptions:	1. The edit feature satisfies the need to test for the ability to make changes, i.e., if edit is denied, then changes are not allowed and vice versa. 2. Data can remain in current repositories (R20). 3. The watermarking capability is one of the policies of the software (R23).

A.2.4.1 Permutations

Actions	Sub-task	Evaluation
A. Perform the following tests as a user who is authorized to have access to the TDP (unless stated otherwise). Section A.1.8 lists the individual policies evaluated.		
A1. List and briefly explain the types of encryption the DRM software implements and where it is used in the system.		
A2. Evaluate whether the DRM software functions, natively, with the file types in the TDP.		

Actions	Sub-task	Evaluation
A3. Evaluate the number of ways policies may be applied to the TDP (i.e., can the policies be applied only when the software's local agent is installed on the workstation where the policies are being applied or can the policies be applied via other methods?)		
A4. Evaluate and list the methods for applying policies.		
A5. Apply each restrictive policy by itself to the TDP, one at a time; then verify that the policy functions as described.	A5.1 Local agent—verify the policy using each file's native application.	
	A5.2 Browser—verify the policy for each file in the browser.	
A6. Apply Policy Set 1 to the TDP; verify the policy set functions as expected.	A6.1 Test using each file's native application.	
	A6.2 Test using the browser for each file.	
A7. Apply Policy Set 2 to the TDP; verify the policy set functions as expected.	A7.1 Test using each file's native application.	
	A7.2 Test using the browser for each file.	
A8. Zip file—Apply Policy Set 1 to the contents of the TDP after it is compressed into a Zip file; verify the policy set functions as expected.	A8.1 Access via WinZip.	
	A8.2 Access via 7-Zip.	
	A8.3 Access via Windows Explorer.	
A9. Zip file—Apply Policy Set 2 to the contents of the TDP after it is compressed into a Zip file; verify the policy set functions as expected.	A9.1 Access via WinZip.	
	A9.2 Access via 7-Zip.	
	A9.3 Access via Windows Explorer.	
A10. As an <i>unauthorized</i> user, attempt to manipulate the TDP for Policy Set 1 and Policy Set 2.	A10.1 Unauthorized users should not have any access permissions.	
A11. Evaluate how a copy of a DRM-protected TDP continues to be protected.	A11.1 Make a copy of the (unchanged) TDP and send it to another person. Does the copy maintain the same level of DRM protections as the original?	
	A11.2 Perform tests for authorized and <i>unauthorized</i> users.	
A12. Evaluate whether DRM protection of a TDP interferes with the routine maintenance process of making backup copies of files. ^a		
A13. Evaluate whether DRM protection of a TDP is compatible with OneDrive or SharePoint or other non-local file store approaches.		
A14. Evaluate revocation.	A15.1 Explore the ability for the software to remove permissions once users have the TDP in their possession.	

Actions	Sub-task	Evaluation
	A15.2 Apply permissions, then revoke them one at a time—testing to ensure the permissions were removed.	
	A15.2 What are the limitations for this functionality?	
A15. Revocation using an expiration date.	A16.1 Test for revocation but use a timeout period after which the permissions are automatically removed.	
A16. Ensure TDP destruction.	A17.1 Explore the possibilities in the DRM software to verify that data has been destroyed.	
A17. Evaluate distribution.	A18.1 Can DLA control distribution of the TDP by preventing or providing distribution permissions to an OEM?	
	A18.2 Evaluate whether the DRM software can prevent OEMs from redistributing the TDP without permission from DLA.	
	A18.3 If the OEM attempts to redistribute the TDP without DLA permission, is DLA notified?	
A18. Ensure TDPs provided by without DRM protections are accessible – i.e. the DRM client does not automatically apply permissions.		

^a These tests specifically refer to the backup process that many companies run in the background in the case of storage failure.

A.2.5 Test Case Set 1.2: Evaluate Advertisement Options

Overview:	Evaluate the options DLA has for advertising the TDP while secured by DRM.
Requirements:	R1
Preconditions:	1. A TDP is available for DLA to advertise a new procurement opportunity to an intended group of OEMs. 2. Authorized and unauthorized user sets exist.
Postconditions:	1. The procurement opportunity is advertised by DLA to OEMs. 2. Authorized OEMs can review the advertised procurement opportunity. 3. Unauthorized OEMs cannot review the contents of the advertised procurement opportunity.
Assumptions:	1. LDAP is configured with authorized users. 2. A way to communicate with a group of authorized OEM users exists through the vendor platform or some external source, such as email or a web portal.

A.2.5.1 Permutations

Actions	Sub-task	Evaluation
A. Evaluate the options DLA has for advertising the TDP while secured by DRM.		
A1. Evaluate the options for DLA to advertise the procurement opportunity. The minimal options follow:	A1.1 Email	
	A1.2 Listing on a website	

Actions	Sub-task	Evaluation
A2. Explore the software to evaluate whether it offers additional options for advertising the procurement opportunity.		
A3. Explore the options for DLA personnel to delay applying DRM to data (e.g., bid packages) until after the final approval steps for the data to be advertised.		
A4. Evaluate the ability for authorized non-DLA users to receive data from DLA securely.		
A5. Evaluate whether a group of authorized OEM users can participate in the procurement opportunity described by a TDP under DRM after DLA has advertised the procurement opportunity through the DRM software solution or an external process.		
A6. Evaluate the ability of the software to allow DLA to confirm receipt of the procurement opportunity advertisement to the intended users.		
A7. Evaluate the ability for security policies and DRM controls to travel with the data successfully.		

A.2.6 Test Case Set 1.3: Transfer Data to Many Users Securely

Overview:	- DLA can transfer data to many users securely, with data protected by DRM. - Data must arrive intact and remain intact. - DRM protection offers security in transit, thwarting interception (data in transit). - DLA can apply access permissions to the data.
Requirements:	R2.1, R2.3, R2.4, R3.1
Preconditions:	The TDP has a policy set applied.
Postconditions:	The TDP has been transferred to two or more users with its policy set intact.
Assumptions:	None

A.2.6.1 Permutations

Actions	Sub-task	Evaluation
A. DLA can transfer data to many users securely, with data protected by DRM. Data must arrive intact and remain intact.		
A1. Evaluate whether DLA can transfer data to many users securely, with data protected by DRM.	A1.1 Evaluate all DRM policy sets per Section A.1.8.	
	A1.2 Email the TDP to several users and ask them to manipulate the TDP in a manner that should be denied by Policy Set 1.	
A2. Evaluate each file in the TDP and confirm that the file received by the OEM is an exact copy of the DLA source file to an acceptable confidence level maintaining that data remains intact. ^a		

Actions	Sub-task	Evaluation
A3. Evaluate features of the DRM software to prevent or detect unauthorized changes after the file is received.		
A4. Evaluate whether DRM protection offers security in transit, thwarting interception (data in transit)	A4.1 Use software, such as Wireshark (https://www.wireshark.org/), to simulate a man-in-the-middle attack. Review this write up for a possible approach: http://worldcomp-proceedings.com/proc/p2011/SAM4991.pdf .	

^a This test notes how often a file is checked for being intact, e.g., the DRM software might check only the first time the user opens a file and never again.

A.2.7 Test Case Set 1.4: Assign Access Permissions to DLA and Non-DLA Users

Overview:	Explore the ability to assign access permissions (policy sets) to groups of non-DLA users for the TDP. Grouping OEMs and then giving them DRM permissions to a TDP would enable DLA to manage access better. DLA can apply unique access permissions by user.
Requirements:	R0.2, R3.3, R5.3, R21
Preconditions:	The non-DLA users are not listed in our LDAP.
Postconditions:	Ideally, the non-DLA users can be assigned specific policy sets but this precondition is yet to be determined.
Assumptions:	The software can assign policy sets to groups of users for a TDP.

A.2.7.1 Permutations

Actions	Sub-task	Evaluation
A. Explore assigning different access permissions to sets of non-DLA users—these users are not listed in LDAP.		
A1. Evaluate whether it's possible to govern access to TDP using a large group of users. For example, User Group A has Policy Set 1 for the TDP while User Group B has Policy Set 2 for the TDP.		
A2. Show that different permissions can be assigned to different groups.	A2.1 Test using each file's native application (with the local agent active).	
	A2.2 Test by accessing the TDP via the browser.	
A3. Explore the possibility of assigning permissions to roles—then assigning those roles to different user groups.	A3.1 Can we assign roles to groups of Non-DLA users? Show that roles with different permissions can be assigned to different groups.	
	A3.2 Test using each file's native application (with the local agent active).	
	A3.3 Test by accessing the TDP via the browser.	

Actions	Sub-task	Evaluation
B. Explore assigning complete access to DLA personnel for DLA-originated data.^a		
B1. Explore whether different permissions and access levels are needed to administer DRM policies or access reports produced by DRM software—a small group of DLA personnel might need different access levels to control administration of DRM.		
B2. Explore whether DLA personnel could place data in the DLA data store without using local agent software.		
B3. Explore whether DLA personnel could access data of other DLA personnel in the DLA data store without restrictions and without using local agent software.		
C. Explore obtaining permission to access the TDP if not initially given access permissions.		
1. Attempt to access a file as a user without access permission. 2. Use functionality built into the DRM software to request permission to access the TDP. 3. Grant access as an administrator. 4. Access the TDP in the limits of the granted privileges.		
C1. Test using each file's native application (with the local agent active).		
C2. Test by accessing the TDP via the browser.		
D. Explore DLA's ability to deny permission to access the TDP.		
D1. The previous tests assume permission is granted when requested. How does the software allow DLA to deny a user's request for access?		

^a To reduce the overall disruption to DLA processes, it is recommended that DRM permissions be assigned even to documents behind DLA's firewall. For example, what if a product data specialist at DLA puts a file in the data store where the public can access it (with DRM permissions), then a potential bidder sends an email to someone at DLA, such as a product specialist (PS), with a question about the data. The normal DLA workflow would allow the other person at DLA, the PS, to grab a copy from the same data store where the OEM got it to respond to the question. The workflow would change if DRM permissions intruded on that process.

A.2.8 Test Case Set 1.5: Policy Automation

Overview:	Explore the system's ability to automatically apply policy sets based on applicable factors. The factors are limited to those allowed by the software.
Requirements:	R26
Preconditions:	The TDP does not have any policies applied, i.e., it's a clean slate.
Postconditions:	The TDP takes on the applicable policies once the trigger criteria for the automation is met.
Assumptions:	Data can remain in current repositories (R20).

A.2.8.1 Permutations

Actions	Sub-task	Evaluation
A. Establish the factors that the software allows for automating the application of a policy set. For example, can the system revoke privileges automatically 30 days after TDP publication?		
B. Establish automation for 3 to 5 of the most likely scenarios and test the capability.		

A.3 Task 2: Transfer Data Securely in Reverse

A.3.1 Purpose

Task 2 tests the basics of DRM, specifically the secure transfer from external parties to DLA. This task tests the ability and options for a non-DLA organization to use DRM to transfer data to DLA securely, and the ability of DLA to receive the data under DRM.

- Transfer data securely to an incoming DLA data store (reverse data transfer) under the following conditions:
 - When the TDP is unchanged
 - When the TDP has been changed only by adding one or more files (e.g., adding a change request form)
 - When the TDP has been modified
 - When a new TDP is created
- Apply DRM policies to a new TDP
 - Evaluate the OEM's ability to place DRM policies on newly generated files
 - Evaluate DLA's ability to intake DRM-protected files that DLA did not create or share
 - Evaluate DLA's ability to remove DRM protections from files received from an OEM (e.g., when the file is placed in DoD's secure perimeter firewall)

A.3.2 Requirements

R9.1, R9.3, R11, R12, R13, R14, R24

A.3.3 Assumptions

- Task 1 has verified that data can be transferred securely using DRM policies. We can assume DRM functions the same way in both transfer directions.
- OEMs only want to protect their TDP; they do not intend to restrict DLA from viewing their packages.
- Change requests—an OEM change request consists of one or more of the following.
 - A file, form, or message sent separately or independently from a TDP.
 - A file or form added to a TDP.
 - A change to one or more files in the TDP.
 - A message or accompanying form explaining the changes.

Note: Although ideally not involved in this process, DLA may assist in administering DRM policy protections on modified TDPs.

A.3.4 Test Case Set 2.1: Transfer Data Securely in Reverse

Overview:	The OEM transfers TDP data to DLA. DLA receives and ingests the data into its systems. DRM security is maintained throughout the process. Data must arrive intact. These tests serve as a continuation of the work from Task 1 and focus on ensuring a baseline in the performance and maturity of the DRM software when data flows in the reverse direction.
Requirements:	R9.1, R9.3, R11, R12, R13, R14, R24
Preconditions:	1. Task 1: Data can be transferred to many users securely. 2. An appropriate policy set is applied to data; authorized and unauthorized user sets exist.
Postconditions:	TDPs arrive at DLA within DRM policy controls and DLA can ingest the data.
Assumptions:	1. A collection of authorized users exists representing OEM users and the central DLA authority. 2. The same level of DRM is applied to data after modification by authorized OEM users.

A.3.4.1 Permutations

Actions	Sub-task	Evaluation
A. Evaluate the ability of the DRM software to transfer and receive data in the TDP in the reverse direction.	A.1 Evaluate the OEM's ability to securely send TDP to DLA.	
	A.2 Evaluated the ability of DLA to receive various forms of TDPs (unchanged to brand new) with DRM protection.	
B. Evaluate each file in the TDP and confirm that the file received by DLA is an exact copy of the file sent by the OEM to an acceptable confidence level.		
C. Test using the local agent: data transfer in the reverse direction when the TDP data is initially delivered to the OEM from DLA.		
C1. Policy Set 1	C1.1 TDP data has experienced no changes.	
	C1.2 TDP data has experienced no changes but the TDP now includes authorized additional data (e.g., adding a change request form).	
	C1.3 TDP data initially delivered to the OEM has experienced authorized changes (e.g., a change request form plus changes to one or more files in the envelope).	
C2. Policy Set 2	C2.1 TDP data has experienced no changes.	
	C2.2 TDP data has experienced no changes but the TDP now includes authorized additional data (e.g., adding a change request form).	
	C2.3 TDP data initially delivered to the OEM has experienced authorized changes (e.g., a change request form plus changes to one or more files in the envelope).	
D. Test using the browser: data transfer in the reverse direction when the TDP data initially delivered to the OEM from DLA.		
D1. Policy Set 1	D1.1 TDP data has experienced no changes.	

Actions	Sub-task	Evaluation
	D1.2 TDP data has experienced no changes, but the TDP now includes authorized additional data (e.g., adding a change request form).	
	D1.3 TDP data initially delivered to the OEM has experienced authorized changes (e.g., a change request form plus changes to one or more files in the envelope).	
D2. Policy Set 2	D2.1 TDP data has experienced no changes.	
	D2.2 TDP data has experienced no changes, but the TDP now includes authorized additional data (e.g., adding a change request form).	
	D2.3 TDP data initially delivered to the OEM has experienced authorized changes (e.g., a change request form plus changes to one or more files in the envelope).	

A.3.5 Test Case Set 2.2: Transfer Data Generated by the OEM in Its Enterprise Securely in Reverse

Overview:	The OEM can initiate or apply DRM policies on new, original-to-the-OEM TDP data.
Requirements:	R13
Preconditions:	- Task 1: Data can be transferred securely to many users. - An appropriate policy set is applied to data; authorized and unauthorized user sets exist.
Postconditions:	The TDP exists within the controls of DRM policy set. DLA did not initiate applying the DRM policy set to data, although DLA assistance may have been needed in applying the DRM policy.
Assumptions:	- A collection of authorized users exists representing OEM users and the central DLA authority. - An appropriate level of DRM can be applied to data created by authorized OEM users.

A.3.5.1 Permutations

Actions	Sub-task	Evaluation
A. Evaluate the ability of the OEM to use DRM software to secure a new, unique-to-the-OEM TDP.		
A1. Evaluate the OEM's ability to secure data without DLA's input.		
A2. Evaluated the ability of DLA to receive data under DRM that has never existed in the enterprise before.		

Actions	Sub-task	Evaluation
B. Test using the local agent: when data is transferred in the reverse direction.		
B1. Policy Set 1	B1.1 The TDP is new data, unique to the OEM, and created for the specific procurement (e.g., a new TDP that has never existed in DLA's systems prior).	
B2. Policy Set 2	B2.1 The TDP is new data, unique to the OEM, and created for the specific procurement (e.g., a new TDP that has never existed in DLA's systems prior).	
C. Test using the browser: when data is transferred in the reverse direction.		
C1. Policy Set 1	C1.1 The TDP is new data, unique to the OEM, and created for the specific procurement (e.g., a new TDP that has never existed in DLA's systems prior).	
C2. Policy Set 2	C2.1 The TDP is new data, unique to the OEM, and created for the specific procurement (e.g., a new TDP that has never existed in DLA's systems prior).	

A.4 Task 3: Transfer Data Securely with Validity Checks

A.4.1 Purpose

- Check the validity of the data in the TDP after the OEM obtains it from the DLA data store.
- Confirm the results of the validity checks to an acceptable confidence level.
- Summarize the mechanism by which the DRM software checks the validity.
 - Who can view the validity checks? Can DLA view that the OEM received an intact copy of the TDP?

A.4.2 Requirements

- R2.2, R4.7

A.4.3 Assumptions

- Task 1 has verified the data and it can be transferred securely using DRM policies.
- A passing validity check indicates that the file received by the OEM is an exact copy of the file from DLA.

A.4.4 Test Case Set 3.1: Check the Validity of Data Transferred from DLA to the OEM

Overview:	An exact copy of the data is transferred and remains identical to the source upon arrival, passing the validity check.
Requirements:	R2.2, R4.7
Preconditions:	Task 1: Data is transferred securely from the DLA data store to the OEM.
Postconditions:	The TDP's validity is known to the software or server.

Assumptions:	1. For permutations involving native application testing, the OEM has installed the DRM platform's local agent and the local agent app is active. 2. A collection of authorized users exists representing OEM users and the central DLA authority. 3. Vendor's DRM policies can be enforced when the native application is used and local agent app is active. The local agent automatically performs the validity check upon receipt before the OEM performs other actions with the data.
---------------------	---

A.4.4.1 Permutations

Actions	Sub-task	Evaluation
A. Evaluate the ability of the DRM software to check the validity of the data in the TDP after it is sent from the DLA data store to the OEM.		
A1. Evaluate each file in the TDP and confirm the results of the validity checks to an acceptable confidence level.		
A2. Evaluate the ability to share the results of validity check with the intended recipients and originators.		
B. Local agent testing—Explore how the DRM platform reports on the validity checking of data that the OEM receives in a TDP using native applications (with the local agent active) for their respective file formats (or the container, e.g., .zip).		
B1. Using a central policy repository server with Policy Set 1 applied, explore the validity checking of newly created and transferred TDP content from the perspective of	B1.1 the DLA administrator, i.e., transaction logs, browser console logs.	
	B1.2 the OEM, i.e., file hashes, Wireshark logs.	
C. Browser application testing—Explore how the DRM platform reports on the validity checking of data that the OEM receives in a TDP (or the container, e.g., .zip) using the browser applications (Chrome, etc.).		
C1. Using a central policy repository server with Policy Set 1 applied, explore the validity checking of newly created and transferred TDP content from the perspective of	C1.1 the DLA administrator, i.e., transaction logs, browser console logs.	
	C1.2 the OEM, i.e., file hashes, Wireshark logs.	
C2. Using a central policy repository server with Policy Set 2 applied, explore the validity checking of newly created and transferred TDP content from the perspective of	C2.1 the DLA administrator, i.e., transaction logs, browser console logs.	
	C2.2 the OEM, i.e., file hashes, Wireshark logs.	

A.5 Task 4: Transfer Data Securely in Reverse with Validity Checks

A.5.1 Purpose

Evaluate the ability of the DRM software to check the validity of the data in the TDP after the OEM sends it to the DLA inbound data store.

- Explore the features for indicating that the file received by the DLA is an exact copy of the file sent by the OEM

- when the TDP has been changed only by adding one or more files (e.g., adding a change request form),
- when the TDP has been modified,
- when the entirely new TDP is created, and
- when original TDP is used, unchanged.
- Explore the features for the following:
 - Does the OEM create validity check data that is sent to DLA for DLA to perform the check?
 - Is validity check data in TDP data package or is validity check data sent separately?
 - Is the OEM informed of the result of the validity check on the data received by the DLA?
- Can DLA view the validity check?
 - Can DLA evaluate the validity check data on its own or must the OEM evaluate and inform DLA of the result?

A.5.2 Requirement

- 9.2

A.5.3 Assumptions

- A collection of authorized users represents OEM users and the central DLA authority.
- Task 1 has verified that data can be transferred securely using DRM policies.
- Task 2 has verified that an OEM can use DRM policies to transfer data securely to DLA.
- DLA's DRM policies have been applied to files modified by the OEM and to files created by the OEM.

A.5.4 Test Case Set 4.1: Check Validity in Reverse

Overview:	Explore the features for indicating that the file received by the DLA is an exact copy of the file sent by the OEM. Explore the features and processes for obtaining validity checks. Explore the features and processes for distributing validity checks, i.e., the visibility of validity checks.
Requirements:	9.2
Preconditions:	Task 2: Data is transferred from the OEM to the DLA data store securely.
Postconditions:	The TDP's validity is known to the software or server; validity check data can be furnished to DLA and available to the OEM.
Assumptions:	Local agent 1. The OEM has installed the vendor's local agent. 2. The local agent automatically initiates the validity check upon receipt of data at DLA, before DLA performs any other actions with the data. Browser: The validity check is initiated automatically upon receipt of data at DLA, before DLA performs any other actions with the data.

A.5.4.1 Permutations

Actions	Sub-task	Evaluation
A. Evaluate the ability of the DRM software to check the validity of the data in the TDP.		
A1. Evaluate each file in the TDP and confirm the results of the validity checks to an acceptable confidence level.	A1.1 What validity checks are performed?	
	A1.2 How are results of the validity checks (pass or fail) indicated?	
	A1.3 When or how often are validity checks performed?	
A2. Evaluate obtaining results of validity checks.	A2.1 Does the OEM create validity check data automatically?	
	A2.2 Are validity checks (pass or fail) performed automatically?	
	A2.3 Does the sender receive validity check results automatically?	
	A2.4 Are validity check results transmitted as a separate communication?	
A3. Evaluate sharing the results of validity checks with both parties, OEM and DLA.	A3.1 Are validity check results passed to DLA automatically?	
	A3.2 Is action needed to send validity check results to DLA?	
	A3.3 Can DLA evaluate validity check results independently?	
A4. Test using the local agent—Policy Set 1 under the following conditions:	A4.1 When the TDP has been changed only by adding one or more files (e.g., adding a change request form).	
	A4.2 When the TDP has been modified.	
	A4.3 When an entirely new TDP is created.	
	A4.4 When the original TDP is used, unchanged, i.e., the OEM did not change the TDP supplied by DLA but is now sending that TDP back to DLA. Can the software check the validity, indicating that the TDP has not been changed?	
A5. Test using the local agent—Policy Set 2 under the following conditions:	A5.1 When the TDP has been changed only by adding one or more files (e.g., adding a change request form). Can the software detect that the TDP now has additional files?	
	A5.2 When the TDP has been modified.	
	A5.3 When an entirely new TDP is created.	
	A5.4 When the original TDP is used, unchanged.	
A6. Test using the browser—Policy Set 1 under the following conditions:	A6.1 When the TDP has been changed only by adding one or more files (e.g., adding a change request form).	
	A6.2 When the TDP has been modified.	
	A6. 3 When an entirely new TDP is created.	
	A6.4 When the original TDP is used, unchanged.	
A7. Test using the browser—Policy Set 2 under the following conditions:	A7.1 When the TDP has been changed only by adding one or more files (e.g., adding a change request form).	
	A7.2 When the TDP has been modified.	
	A7.3 When an entirely new TDP is created.	
	A7.4 When the original TDP is used, unchanged.	

A.6 Task 5: Collect Forensic Information and Check the Identity of the Recipient

A.6.1 Purpose

This set of test cases evaluates the DRM software's breadth of forensic capabilities, including the following:

- Control access to the TDP.
- Local agent—Identify (who, when, and where) file accesses and changes.
- Browser—Identify (who, when, and where) file accesses and changes.
- Carry logging forward when accessing a copy of the TDP.
- Supply information about changes.
- Check identity and validity concurrently.
- Report on user behavior.
- Support an investigation by furnishing data in a report format.

When applicable, the functionality is tested in the browser and with the local agent using each TDP file's native application software.

A.6.2 Requirements

R2.2 + R9.2 (currently), R4.1–R4.7, R5.1, R6.1, R6.2, R6.3, R10, R15, R22, R25

R0.2—auditing

A.6.3 Assumptions

- Data is transferred from a controlled DLA file store to the OEM.
- For Test Case Sets 5.2 and 5.6 only, data is transferred from OEM to an incoming DLA data store also.
- The OEM takes no actions to supply the identity check.

A.6.4 Test Case Set 5.1: Control Access to the TDP

Overview:	An OEM currently only needs a CAGE code to log in and access the TDP on DLA's Internet Bid Board System (DIBBS) website. Explore the ability for DLA to use the software to control who can obtain the data. For example, when DLA posts the TDP on DIBBS for distribution, does the software offer any controls to limit who can obtain the data?
Requirements:	R5.1
Preconditions:	None, this set of test cases explores the capabilities of the DRM software.
Postconditions:	Only authorized user can access the TDP.
Assumptions:	Task 1 has been completed.

A.6.4.1 Permutations

Actions	Sub-task	Evaluation
A. Repository Control		
A1. Evaluate whether the software can store files with their access governed by the permissions one has in the software.		
A2. Evaluate whether the software can govern the access to files in another specified location (e.g., data can remain in its current repositories) by the permissions one has in the software.		
B. Roles		
B1. Evaluate whether the software can assign roles to non-DLA members.	B1.1 Is it possible to loop OEMs into DLA's circle of trust and assign one or more roles to an OEM? This would enable the OEM access to only those TDPs that fall in its purview.	
B2. If roles can be assigned to non-DLA members, work with the team to set up a demonstration.	B1.2 Can the software control the types of TDP an OEM can access, e.g., radar antennas?	

A.6.5 Test Case Set 5.2: Local Agent—Identify Who, When, and Where

Overview:	The TDP can be accessed from a native application using the local agent. These test cases explore the information from the DRM software. Discover the types of information the software can provide, such as the following: • Who accessed or attempted to access the TDP? • Who made changes to or attempted to make changes to the TDP? • When was the TDP accessed or attempted? • When were the changes made or attempted? • Where was the TDP accessed or attempted? • Where were the changes made or attempted? Test cases are evaluated using Policy Set 1 and 2.
Requirements:	R4.3, R4.4, 4.5, 4.6, R6.2, R25
Preconditions:	The TDP is available to be accessed, a policy set is applied to the TDP, and authorized and unauthorized user sets exist.
Postconditions:	The access log is updated showing information for the actions performed on the TDP.
Assumptions:	Tasks 1 and 3 have been completed.

A.6.5.1 Permutations

Local Agent Test Cases

Execute the following test cases as authorized and unauthorized users.

Actions	Sub-task	Evaluation
A. Explore the ability for DLA to track who receives protected data.		
A1. When the OEM attempts to access the TDP, does the software send a notification with the identity of the user making the attempt?		
A2. If a notification is sent, what kinds of information are provided?		
B. While the TDP is remote, i.e., located with the OEM, explore the software's ability to do the following:		
B1. Determine who attempts to access the TDP.		
B2. Determine who is making the changes.		
B3. Determine who attempted to make changes but was denied by the system.		
B4. Determine when the changes are made.		
B5. Determine where (geographic location) the changes occur.		
B6. Determine the application used to access or manipulate the TDP.		
B7. Determine how often information is sent back to DLA, e.g., is a log sent each time a file is saved and when the file is closed?		
C. Once the TDP is transferred to DLA, explore the software's ability to do the following. More information may be gained from the file once it's back with DLA.		
C1. Determine who made the changes.		
C2. Determine when the changes were made.		
C3. Determine where (geographic location) the changes occurred.		

Local Agent

The following test cases explore the information gathering capacities of the local agent. When evaluating with the local agent, use the following delivery methods as an authorized and unauthorized user.

1. Download using the DLA website (Method 1)
2. Email (Method 3)

Each test case must be evaluated using Policy Set 1 and 2.

Local Agent—Disconnected from the Internet

Explore the local agent's capabilities when the user is not connected to the internet. Evaluate using the same delivery methods as described in 6.1.1.2.

Actions	Sub-task	Evaluation
A. When not connected, what does the local agent allow the user to do?		
A1. Can the local agent authenticate the user when not connected?		
A2. Can the user authenticate while connected, then disconnect and continue working with the files? What are the limitations to what the user can do while disconnected?		

Actions	Sub-task	Evaluation
B. Since logging information can only be sent if the user is connected to the internet, explore the capabilities of the local agent to store logging information and then provide that information once a connection is restored.		
B1. Can the local agent detect when its log has been deleted or altered? Does the local agent receive acknowledgement that its log was received and accepted?		

A.6.6 Test Case Set 5.3: Browser—Identify Who, When, and Where

Overview:	The TDP can be accessed through a browser. These test cases explore the information from the DRM software when the TDP is accessed through the browser. Discover the types of information the software can furnish: • Who accessed or attempted to access the TDP? • Who made changes to or attempted to change the TDP? • When was the TDP accessed or the attempt to access made? • When were the changes or attempted changes made? • Where was the TDP accessed or attempted? • Where were the changes or attempted changes made?
Requirements:	R6.1, R6.2, R6.3, R25
Preconditions:	The TDP is available to be accessed, the policy set is applied to the TDP, and authorized and unauthorized user sets exist.
Postconditions:	The access log is updated showing information for the actions performed on the TDP.
Assumptions:	Tasks 1 and 3 have been completed.

A.6.6.1 Permutations

Actions	Sub-task	Evaluation
A. Explore DLA's ability to track who accesses the protected data in the browser.		
A1. When the OEM attempts to access the TDP, does the software log a notification with the identity of the user making the attempt?		
A2. What kinds of information are logged when the TDP is accessed through the browser?		
A3. Who is attempting to access the TDP?		
B. While the TDP is being manipulated in the browser, explore the software's ability to do the following:		
B1. Determine who is making the changes.		
B2. Determine who attempted to make changes but was denied by the system.		
B3. Determine when the changes occurred.		
B4. Determine where (geographic location) the changes occurred.		
B5. Determine how often information is logged.		

Execute the test cases as authorized and unauthorized users.

A.6.7 Test Case Set 5.4: Access a Copy of the TDP

Overview:	In these test cases, an unauthorized user has received a copy of the TDP. For example, the TDP was forwarded to the user through email. This user does not have a local agent and is attempting to access the TDP using native applications as well as through the browser. Perhaps the TDP can't be viewed at all without local agent; can this user get local agent? Does the software supply the same level of logging for a copy sent to an unauthorized person?
Requirements:	R15
Preconditions:	1. A copy of the TDP has been forwarded, via email, to an unauthorized user. 2. Policy Set 2 has been applied to the TDP.
Postconditions:	The system's log files have been updated with all the possible information.
Assumptions:	Tasks 1 and 3 have been completed.

A.6.7.1 Permutations

Actions	Sub-task	Evaluation
A. As an unauthorized user, attempt to do the following.		
A1. View all the files in the TDP.		
A2. Change each file in the TDP.		
A3. Screenshot one or more files.		
A4. Print one or more files.		
A5. Attempt to share screen over Zoom or MS Teams.		
A6. Take a photo of the screen using a camera or cell phone.		
A7. Evaluate whether the same level of logging occurs when a copy of the TDP is sent to an otherwise authorized person, instead of that authorized person obtaining the TDP from DLA.		
A8. Evaluate whether the routine maintenance process of making backup copies of files produces access log entries or entries in a log of copies made.		
A9. Evaluate whether logging is compatible with indexing or background processes for OneDrive, SharePoint, or other non-local file store approaches.		

A.6.8 Test Case Set 5.5: Supply Information about Changes

Overview:	Explore the ability of the DRM software to detect the changes made to the TDP. Once the change is identified, is enough information provided to help evaluate the seriousness of the changes made to the TDP?
Requirements:	R4.1, R4.2, R4.6
Preconditions:	The original unchanged TDP has DRM Policy Set 2 applied.
Postconditions:	The TDP has been changed and the change has been reported.
Assumptions:	Task 1 has been completed.

A.6.8.1 Permutations

Actions	Sub-task	Evaluation
A. Evaluate whether the DRM software can detect the changes made to the TDP.		
A1. For example, if the TDP is opened and a paragraph in one of the documents is modified—can the software point out the change?		
A2. If the software does not have that capability, does an alternative method provide this information?		
B. Discover if DLA can uncover the seriousness of the change.		
B1. Evaluating the seriousness of a change requires in-depth knowledge of the contents of the TDP. If given enough information, an SME can interpret the effect the change has on the system, part, etc.		
B2. For example, removing the firing pin from the schematic of a rifle is likely to leave the weapon unusable and would, therefore, be a serious change but an alteration to the fabric for the rifle's sling may be minor.		

A.6.9 Test Case Set 5.6: Check Identity and Validity Concurrently

Overview:	Verify that the software can perform identity checks (Task 5) and validity checks (Task 3) at the same time.
Requirements:	R9.2 (validity checks) + R2.2 (validity checks) currently + R6.1, R6.2, R10 (identity checks)
Preconditions:	- Policy Set 1 has been applied to the TDP. - The TDP is posted on a website and can be readily downloaded.
Postconditions:	- The system can provide the identity of the user. - The DLA receives an indication (a validity check) that the file delivered to the OEM user is correct.
Assumptions:	Tasks 1 and 3 have been completed.

A.6.9.1 Permutations

Actions	Sub-task	Evaluation
A. With the local agent, as an authorized and unauthorized user, do the following.		
A1. Download the TDP to your local machine.		
A2. Open the TDP using its native applications.		
A3. Describe the information given about the identity of the user.		
A4. Describe the validity check information given to DLA, the OEM, or both.		
B. Through the browser, without the local agent, as an authorized and unauthorized user, do the following.		
B1. Download the TDP to your local machine.		
B2. Open the file TDP using your browser.		
B3. Describe the information given about the identity of the user.		
B4. Describe the validity check information given to DLA, the OEM, or both.		

A.6.10 Test Case Set 5.7: Report on User Behavior

Overview:	Baked-in usage tracking and analytics: the platform tracks user activities and behavior patterns for analytics.
Requirements:	R22
Preconditions:	The software is set and can access the TDP on which it monitors user behavior.
Postconditions:	N/A
Assumptions:	Tasks 1 and 3 have been completed.

A.6.10.1 Permutations

Actions	Sub-task	Evaluation
A. How must the DRM software be set to gather behavior information? For example, must the TDP be stored in the DRM vendor's own datastore or can behavior information be gathered when the TDP is in DLA's network or the OEM's network?		
B. Explore and explain the types of activities and behavior tracked when accessing the TDP.		
C. Explore and explain the types of analytics from the software when accessing the TDP.		
D. Are reports describing possible unauthorized behavior available?		
E. Does the system send alerts when odd behavior is detected?		

A.6.11 Test Case Set 5.8: Support Investigation

Overview:	Describe the ability to support a forensic investigation with reports, logs, etc. For example, can the software report on who, what, when, and where logs were generated for a single TDP rather than the user gathering information from various locations into an ad hoc report?
Requirements:	R4.7, R0.2—auditing
Preconditions:	1. The TDP has been accessed by authorized and unauthorized users. 2. The TDP has been modified by authorized users.
Postconditions:	Unchanged (logs have been examined).
Assumptions:	Logs are available in the system for reports.

A.6.11.1 Permutations

Actions	Sub-task	Evaluation
A. List the data that can be extracted from the system.		
A.1. For an authorized user		
A.2. For an unauthorized user		
B. List the formats in which the data can be given. Is the creation of an ad hoc report required or can a single report or reports supply the necessary information?		
A.1. For an authorized user		
A.2. For an unauthorized user		

Actions	Sub-task	Evaluation
C. Explore how reports are organized: by file? by user? by date? by location? Can reports be filtered and pivoted as a spreadsheet?		
A.1. For an authorized user		
A.2. For an unauthorized user		

A.7 Task 6: DRM Software Information

A.7.1 Purpose

This task explores broad and high-level questions about the potential of DRM software implementation at DLA.

- Decide the support level for a large user base, specifically the number of files that can be under DRM at any time.
- Explore integrating the DRM software with DLA systems—specifically DIBBS.
- Explore the DRM software's ability to accommodate DLA processes.

A.7.2 Requirements

R17, R18, R19

A.7.3 Assumptions

None

A.7.4 Test Case Set 6.1: Integration

Overview:	This test case asks broad and high-level questions about the potential of DRM software implementation at DLA.
Requirements:	R17, R18, R19
Preconditions:	The tester has access to the DRM software and its documentation, and can reach out to the vendor, if needed.
Postconditions:	The tester answered the questions posed in this test case set.
Assumptions:	The tester reviews the DRM software documentation or discusses with the vendor to answer the questions in this test case set properly.

A.7.4.1 Permutations

Actions	Sub-task	Evaluation
A. Explore the ability for the DRM software to support a large user base. A large user base involves TDPs being accessed by OEMs, not users applying DRM permissions.		
A1. Verify that scaling up the platform to meet DLAs needs would not pose a significant challenge. DLA publishes tens of thousands of items each month for procurement processing. Of the over 200,000 manufacturing firms in the United States, each may want to review a large number to TDPs per month.		
A2. Can the system handle DRM for so many TDP accesses over several years—e.g., 20 million accesses per month = 100 lookers (potential bidders) × 7,000 procurement opportunities per day × 30 days per month?		

Actions	Sub-task	Evaluation
B. Explore the ability for the DRM software to integrate with DLA systems.		
B1. How easily can the DRM software pair with DLA's enterprise systems? The assumption is for DLA administrators to apply DRM policies to the TDP prior to posting it in DIBBS.		
B2. Can DRM software integrate with DLA systems (DIBBS) in other ways?		
C. How does the implementation of DRM affect DLA processes? Would implementation significantly affect DLA processes and operations?		
C1. The relevant processes are described in the project's as-is documentation.		

Appendix F

Results of Prototype

As mentioned in Chapter 3, we evaluated our prototype's ability to achieve the 51 requirements identified for securing TDPs (see Appendix D). This was done by systematically evaluating the prototype's ability to carry out the 176 sub-tasks and tasks outlined in the Test Cases (see Appendix E).

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

Overview:	Evaluate how the policies function in practice. Pay specific attention to the policy definitions and the verification of those definitions. For example, if a policy to prevent editing is applied, then the assumption is no edits are allowed. In addition, the test cases explore revoking access once it is granted to a user.
Requirements:	R0.2, R3.2, R5.2, R6.4, R6.5, R7.1, R7.2, R8, R15, R16, R20, R23, R26
Preconditions:	1. The Technical Data Package (TDP) is available as a PDF and ZIP file. 2. The TDP does not have any policies applied. In other words, it is a clean slate.
Postconditions:	Each DRM policy from the software has been tested in the local agent and the browser.
Assumptions:	▪ The edit feature satisfies the need to test for the ability to make changes; if edit is denied, then changes are not allowed and vice versa. ▪ Data can remain in current repositories (R20). ▪ The watermarking capability is one of the policies of the software (R23).

Permutations

1.1.A Perform the following tests as a user who is authorized to have access to the TDP (unless stated otherwise). Section A.1.8 lists the individual policies evaluated.

1.1.A.1 List and briefly explain the types of encryption the DRM software implements and where it is used in the system.

Encryption of data under DRM is applied in transit, at rest, and in use if the file format is of a type supported in a native editor (Microsoft Word, for example). The primary encryption algorithm used is AES 256-bit.

Encryption occurs when a file is added to the system in one of several ways:

1. The file is of a file type configured to be automatically protected/encrypted by Fasoo DRM
2. The file was moved or created in a folder that is configured to automatically protect/encrypt all content contained therein
3. The file was manually placed under Fasoo DRM as a single action

From their Helpdesk Frequently Asked Questions (FAQ):

Fasoo uses Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules to meet the requirements of organizations that are part of or do business with the United States government. They meet the requirements of the Cryptographic Module Validation Program (CMVP) run by the United States National Institute of Standards and Technology (NIST). Documents are encrypted with Advanced Encryption Standard (AES) algorithms. Metadata and logs use Rivest Cipher 4 (RC4) and document keys use RSA certificates.¹

1.1.A.2 Evaluate whether the DRM software functions natively, with the file types in the TDP.

Background: Fasoo FED software offers two encryption categories: (1) its default category for non-computer-aided design (CAD) file types and (2) another, "NX", category specifically for CAD file types. The EDRM software has settings for specifying which file types or file extensions can be encrypted in each category.

When a CAD file type is selected manually for encryption, the user has the default encryption option and an additional option of choosing to use the NX encryption. In contrast, when a non-CAD file is selected manually for encryption, only the default category is presented in the context menu.

Changes to Test Environment: For testing CAD file types, we had planned to use AutoDesk Fusion 360 CAD software, but we found that AutoDesk Fusion software is not listed in the DRM software's current FED_App_Compatibility spreadsheet. We also found that the Fusion CAD software product is oriented toward cloud-based technical data creation and storage, functionality that created obstacles when creating transportable files that would be protected under Fasoo DRM software. We transitioned to SolidWorks 2020 CAD software for our testing, because the SolidWorks software is more file oriented. Using a different CAD software is not expected to affect operation of the EDRM software so long as the CAD software creates and

¹ RSA stands for the last names of the inventors of the RSA algorithm used to encrypt and decrypt data (Rivest, Shamir, and Adleman). An RSA certificate refers to the use of the algorithm to perform the encryption and decryption.

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

stores data within the environment in which EDRM operates, and so long as the software application is supported by the specific EDRM solution. These changes from the Test Plan only apply to Action A2.

Changes to CAD Files being used for testing (TDP for testing): For the 3D CAD file section of testing, we had planned to launch testing from the 3D PDF file in the TDP for testing and use it as the basis for a collection of different CAD file types or formats. It turned out that the version of SolidWorks CAD software we were using was unable to import a 3D PDF file without additional software products. Instead of obtaining the additional products, we used a collection of CAD files that were created for a previous project. Those files depict the same or similar part to the part shown in the 3D PDF file in the TDP for testing. These changes from the Test Plan only apply to Action A2.

Note on terminology: because the 3D PDF file in the TDP for testing could not be imported into SolidWorks CAD software, we are not considering a 3D PDF file to be a 3D CAD file, even though a 3D PDF file does contain 3D geometry data.

Method and Results: For this section of the test, the NX encryption option was exercised when available, in addition to testing the default encryption option. If a CAD file type was generated and the NX encryption type was not presented as an option by Fasoo, standard encryption was tested. For example, some model-based file types tested were not identified by Fasoo as candidates for NX type encryption. See Action 1.1.A.6.1 where testing with a .STEP file was successful, Action A3 where .stl files were successfully encrypted, and Test Case Set 1.5, Action B where a .stl file was successfully encrypted.

First, testing attempted to use the NX option to encrypt both 3D file types in the demonstration's TDP for testing (file types .STEP, and .stl). Results for these file types are given in the table below. Second, testing attempted to use the NX option to encrypt the 3D file types in the collection of files in folder CAD-Test-Data. Results for these file types are also given in the table below. Next, the 3D CAD file that was imported into SolidWorks was exported in different CAD formats with new file extensions but with similar names. For example, linkSidePlate.SLDPRT was saved as linkSidePlate.ext, where .ext is the file extension corresponding to the format of the file exported. (.SLDPRT for SolidWorks part file format.)

Note: unlike the files in the TDP for testing, which are documented in the Software Test Plan (see section 1, Testing References), the exported files were not saved onto SharePoint or otherwise preserved. The rationale for this is that these files contain the same data as the .SLDPRT file, only in a different format. They can be recreated any time from the .SLDPRT file using SolidWorks software.

Table A2.1: Fasoo Encryption for Various Filetypes details the results of the encryption testing for the model-based file types present in the TDP and exported by the standard installation of SolidWorks 2020. The first column names the file type while the second column identifies the source of the file type, the third tracks whether Fasoo could offer NX type encryption on the file type, and the last column tracks whether the default Fasoo encryption could be applied to the file. Notice that nowhere is the default option not supported where the NX option is supported.

Table A2.1: Fasoo Encryption for Various Filetypes

3D Model Filetype	Source ²	NX Type Encryption	Default Encryption
.SLDPRT (Solidworks)	CTD	Yes	Yes
.SLDDRW (Solidworks)	Export	Yes	Yes
.SLDASM (Solidworks)	Export	Yes	Yes
.3dxml 3D XML files	Export	Not supported	Not supported
.3mf 3D Manufacturing Format	Export	Not supported	Not supported
.amf Additive Manufacturing Format	Export	Not supported	Not supported
.CATPart	CTD	Yes	Yes
.ipt Autodesk Inventor Part	CTD	Yes	Yes
.f3d Autodesk Fusion Fusion Part	TDP	Yes	Yes
.sat ACIS files	Export	Yes	Yes
.cgr CATIA Graphics files	Export	Not supported	Not supported
.x_t Parasolid files	Export	Yes	Yes
.x_b Parasolid files	Export	Yes	Yes

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

.prt.1 Pro/ENGINEER and Creo Parametric files	CTD	Not supported	Yes
.jt Jupiter Tessellation	CTD	Yes	Yes
.step Step files	Export ³	Not supported	Yes
.igs	CTD	Yes	Yes
.stl STL files	TDP	Not supported	Yes
.prc	CTD	Yes	Yes
.dwg	CTD	Yes	Yes

Siemens NX CAD files, such as file type .prt were not tested; the Siemens NX Part file, file type .prt, in the CAD Test Data folder was not used. Siemens NX CAD software is not listed in the DRM software's current FED_App_Compatibility spreadsheet, while Siemens Teamcenter software is listed (Teamcenter is the PLM software product offered by Siemens). SolidWorks software does not read or export Siemens NX CAD files. Other CAD software also create output files with a .prt file extension: Solidworks Part, CADKEY files, ProE/Creo Part, Unigraphics/NX files; none of these other .prt file formats were tested either.

The CREO compressed view file, file type .pvz, in the CAD Test Data folder was not tested.

While SolidWorks software has the capability to export CAD images into image file types, such as .jpg files; these would be images or renderings of the CAD data and are not 3D CAD files - these image file types were not tested here.

This testing was completed before Adobe applied an update to its 64-bit version of Adobe Reader software, which resulted in difficulties described in 1.1.A.7.1.

During testing, the CAD software only seemed capable of operating on unencrypted parts. Once Fasoo protection was applied, the following error messages appeared when SolidWorks was directed to open encrypted (whether NX type or default type) files:

SOLIDWORKS



The file CAD File for Testing - Test A2.SLDPRT is corrupt and cannot be opened or repaired.

Please retrieve a back-up copy of the file. If corruptions continue, please contact your local SOLIDWORKS support representative for help in troubleshooting this problem.

OK

✕ No exceptions to this error were found.

This is expected; the version of SolidWorks software available for this testing is SolidWorks CAD software 2020 SP04, which is not listed in the DRM software's current FED_App_Compatibility spreadsheet. Other versions of SolidWorks, such as SolidWorks 2017, are listed in the compatibility spreadsheet, but no other version of SolidWorks was obtained for this testing.

For all other file types that may be found in a TDP (which includes .pdf, .docx, and .pptx), the DRM software operated as expected. That is, they could be encrypted using the

default encryption, but the option to encrypt them using NX encryption was not available. These other filetypes were tested using their respective application software, e.g., SolidWorks CAD software was not used to open and view a .pptx file.

Note: while a 3D PDF file contains 3D geometry data, the option to encrypt a .pdf file using NX encryption was not available.

1.1.A.3 Evaluate the number of ways policies may be applied to the TDP (i.e., can the policies be applied only when the software's local agent is installed on the workstation where the policies are being applied or can the policies be applied via other methods?)

² "TDP" means included in TDP for testing, "CTD" means obtained from folder CAD-Test-Data, and "Export" means created using Save As/export function of SolidWorks CAD software.

³ Although the TDP for testing contains a .step file, that file was not used here; SolidWorks CAD software has the capability for exporting 2 types of .step files and both types were created by export then tested here.

Note: 2 versions of .STEP file type were tested, an AP203 version output by SolidWorks software and an AP214 version output by SolidWorks software. Results are the same for both types.

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

For Fasoo-FED:

Policies are applied only when the user is logged in to the software's local agent installed on the workstation where the policies are being applied. Policies do not appear to be applied when the user is not logged in to the software's local agent, although without being logged in to the software's local agent, and without the proper permissions, the user cannot access files that have had policies applied to them.

Another situation could be a policy applied to a data store. There are three methods of applying encryption to a file:

1. Manual
2. Automatic by file extension when the file is initially created by the native application.
3. Auto encryption
 - Folder(s) can be targeted to encrypt files with specific file extensions as soon as they are added.
 - Folder(s) can be targeted to encrypt files with specific file extensions on a specific schedule.

When logged in as user Imidev1, when files named .stl are pasted into a folder on the EC2, they are encrypted automatically.

When logged in as user MartinDLA, when files named .stl are pasted into a folder on the EC2, they are not encrypted automatically.

When logged in as user MartinDLA, when a file named .stl is selected with <right click>, the menu item "create secure document" appears; I was expecting "create secure NX document"

Note: The Fasoo FED product does not implement browser-based functionality.

1.1.A.4 Evaluate and list the methods for applying policies.

Policies are applied using something called a "permission rule," which describes who can use a document under a particular set of circumstances. A permission rule is defined by the combination of file aspects listed below. These are:

1. Document class
 - The "document class" is a title used to describe a category of documents.
 - All other file aspects are tied to the document class.
 - A document is assigned a document class.
 - A document class can have different permissions for different categories of users, of ownership, and of login status.
2. Intended users (i.e., the party to which permissions or limitations will apply)
 - User groups or individual users
3. Ownership, which identifies the owner of a file. File ownership is assigned using the Fasoo client software. The types of ownership include:
 - The ownership of a document is defined in relation to the document owner.
 - Company document (all documents existing within an organization, no matter who the owner is)
 - My document (the documents that I own)
 - Group's document (the documents owned by a member of my group)
 - Direct supervisee's document (the documents owned by a member of the group where I am the head of the group).
4. Login status
 - Online
 - Offline
 - Personal computer (PC) checkout
5. Permission level
 - Groups of permissions (or lack thereof)
 - For example, a Permissions Level called "Printing" could allow a user to view and print a document, but not edit or execute any other action.

The following is an example of a permissions rule:

4. Document Class: Confidential
5. Intended Users: Original Equipment Manufacturer (OEM) (a user group)
6. Ownership: Company (someone else created the document)
7. Login status: Online, offline, and PC checkout
8. Valid period: Unlimited

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

9. Permissions Level: Restricted printing

In other words, when a user within the OEM group is online/offline/(has file PC checked out) opens a file assigned the Confidential document class created by someone else in the company, they are able to execute all the actions allowed by the Restricted Printing permission level.

For this testing, every permission rule created covered all three options for Login Status: online, offline, and PC checkout, as shown in the above example.

1.1.A.5 Apply each restrictive policy by itself to the TDP, one at a time; then verify that the policy functions as described.

1.1.A.5.1 Local agent—verify the policy using each file's native application.

It is possible to apply the policies one at a time, but the process would be extremely time consuming. Instead, the three different policy sets (Proprietary, Official Use, and Confidential) were applied to each document type (i.e., file type) in Test Case 1.1.A.7.1. This test case is using the results from that test case. Each policy set functions as expected. However, the PDF file types required using a 32-bit version of Adobe Reader software (see 1.1.A.6.1, section about file DRM001.pdf). When using a 64-bit version of Adobe Reader software, the PDF file types could not be opened once the file was encrypted (see 1.1.A.7.1 for details).

1.1.A.5.2 Browser—verify the policy for each file in the browser.

The Fasoo FED product does not implement browser-based functionality.

1.1.A.6 Apply Policy Set 1 to the TDP; verify the policy set functions as expected.

1.1.A.6.1 Test using each file's native application.

Manually assigned the following document classes to each type of file using the DLA user User1DLA.

1. Proprietary
2. Official use
3. Confidential

Used the following files from our Test Data (note: results of the test for each file type are listed as a sub-bullet):

Using file as User1DLA (Owner)

- 10.3D PDF – DRM001.pdf
 - 3D model requires using 32-bit version of Adobe Reader software (see below, section about file DRM001.pdf)
 - 3D model did not open correctly when using 64-bit version of Adobe Reader software (see 1.1.A.7.1 for additional details).
- 11.PDF – Solicitation.pdf
 - Requires using 32-bit version of Adobe Reader software (see below, section about file Solicitation.pdf)
 - Did not open correctly when using 64-bit version of Adobe Reader software (see 1.1.A.7.1 for additional details).
- 12.DOCX – Air_Drop_Platform_Rigging_Manual.docx
 - Proprietary
 - Correctly had full control of the document
 - Official Use
 - Correctly had full control of the document
 - Confidential
 - Correctly had full control of the document
- 13.XLSX – Link_Assembly_Bill_Of_Material.xlsx
 - Proprietary
 - Correctly had full control of the document
 - Official use
 - Correctly had full control of the document
 - Confidential
 - Correctly had full control of the document

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

14.PPTX - Sample_Acceptable_3D_TDP.pptx

- Proprietary
 - Correctly had full control of the document
- Official use
 - Correctly had full control of the document
- Confidential
 - Correctly had full control of the document

15.CAD File for Testing - linkSidePlate.STEP

- Proprietary NX
 - Correctly had full control of the document
 - Opened in Notepad
- Official Use NX
 - Correctly had full control of the document
 - Opened in Notepad
- Confidential NX
 - Correctly had full control of the document
 - Opened in Notepad

Using file as User3DLA (owner)

16.3D PDF – DRM001.pdf (EC2 user user7 on Server C, using 32-bit version of Adobe Reader software, logged in to Fasoo as userID User3DLA)

- 3D model loaded correctly, before encrypting file,
- Closed file, closed Adobe, then used right-click to create secured document as Confidential document class. Using right-click shows all permissions selected.
- There is a lock image on icon of this encrypted file,
- Adobe read the encrypted file, 3D model loaded correctly,
- In Adobe, file has print, save as, and snipping tool permissions.

17.PDF – Solicitation.pdf (EC2 user user7 on Server C, using 32-bit version of Adobe Reader software, logged in to Fasoo as userID User3DLA)

- File loaded correctly, before encrypting file,
- Closed file, closed Adobe, then used right-click to create secured document as Confidential document class. Using right-click shows all permissions selected.
- There is a lock image on icon of this encrypted file,
- Adobe read the encrypted file, file loaded correctly,
- In Adobe, file has print, save as, and snipping tool permissions.

Using file with no User ID

18.3D PDF – DRM001.pdf (EC2 user user7 on Server C, using 32-bit version of Adobe Reader software, not logged in to Fasoo)

- There is a lock image on icon of this encrypted file,
- Using right-click shows Fasoo error, “You do not have permission to view this file.”
- After closing file, closing Adobe, and logging out of Fasoo, tried to open file. Adobe runs and shows an error “Access denied” in addition to the Fasoo error “You do not have permission to open this file.”

19.PDF – Solicitation.pdf (EC2 user user7 on Server C, using 32-bit version of Adobe Reader software, not logged in to Fasoo)

- There is a lock image on icon of this encrypted file,
- Using right-click shows Fasoo error, “You do not have permission to view this file.”
- When trying to open file, Adobe runs and shows an error “Access denied” in addition to the Fasoo error “You do not have permission to open this file.”

Using file as User2DLA (Not the owner)

20.3D PDF – DRM001.pdf (EC2 user user7 on Server C, using 32-bit version of Adobe Reader software, logged in to Fasoo as userID User2DLA)

- Using right-click shows all permissions selected.
- Adobe read the encrypted file, 3D model loaded correctly,
- In Adobe, file has print, save as, and snipping tool permissions.

21.PDF – Solicitation.pdf (EC2 user user7 on Server C, using 32-bit version of Adobe Reader software, logged in to Fasoo as userID User2DLA)

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

- Using right-click shows all permissions selected.
- Adobe read the encrypted file, file loaded correctly,
- In Adobe, file has print, save as, and snipping tool permissions.

Using file as User1OEM (Not the owner)

- 22.3D PDF – DRM001.pdf
- 3D model requires using 32-bit version of Adobe Reader software (see above section about file DRM001.pdf)
 - 3D model did not open correctly when using 64-bit version of Adobe Reader software (see 1.1.A.7.1 for additional details).
- 23.PDF – Solicitation.pdf
- Requires using 32-bit version of Adobe Reader software (see above section about file Solicitation.pdf)
 - Did not open correctly when using 64-bit version of Adobe Reader software (see 1.1.A.7.1 for additional details).
- 24.DOCX – Air_Drop_Platform_Rigging_Manual.docx
- Proprietary
 - Cannot currently print without the Fasoo Smart Print module being installed on our client software.
 - Official use
 - Correct - Permissions restricted to that of an OEM user
 - Confidential
 - Correct - Permissions restricted to that of an OEM user
- 25.XLSX – Link_Assembly_Bill_Of_Material.xlsx
- Proprietary
 - Printing with watermark not included
 - Official use
 - Correct - Permissions restricted to that of an OEM user
 - Confidential
 - Correct - Permissions restricted to that of an OEM user
- 26.PPTX - Sample_Acceptable_3D_TDP.pptx
- Proprietary
 - [Printing w/ watermark not included]
 - Official use
 - Correct - Permissions restricted to that of an OEM user
 - Confidential
 - Correct - Permissions restricted to that of an OEM user
- 27.CAD File for Testing - linkSidePlate.STEP
- Proprietary
 - Printing with watermark not included
 - Opened in Notepad
 - Official use
 - Correct - Permissions restricted to that of an OEM user
 - Opened in Notepad
 - Confidential
 - Correct - Permissions restricted to that of an OEM user
 - Opened in Notepad

Using file as User3OEM (Not the owner)

- 28.3D PDF – DRM001.pdf (EC2 user user7 on Server C, using 32-bit version of Adobe Reader software, logged in to Fasoo as userID User3OEM)
- There is a lock image on icon of this encrypted file
 - Using right-click shows that only View permission is available.
 - Adobe read the encrypted file, 3D model loaded correctly,
 - In Adobe, file does not have print, save as, or snipping tool permissions.
 - Viewing attachments in the 3D PDF was not permitted under “View only” access (based on pretest experience, but a repeat test was not attempted in this sequence)

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

29.PDF – Solicitation.pdf (EC2 user user7 on Server C, using 32-bit version of Adobe Reader software, logged in to Fasoo as userID User3OEM)

- There is a lock image on icon of this encrypted file
- Using right-click shows that only View permission is available.
- Adobe read the encrypted file, file loaded correctly, and
- In Adobe, file does not have print, save as, or snipping tool permissions.

1.1.A.6.2 Test using the browser for each file.

The Fasoo FED product does not implement browser-based functionality.

1.1.A.7 Apply Policy Set 2 to the TDP; verify the policy set functions as expected.

1.1.A.7.1 Test using each file's native application.

Manually assigned the following document classes to each type of file using the OEM user User1OEM.

1. Proprietary
2. Official use
3. Confidential

Used the following files from our Test Data (note: the results of the test for each file type are listed as a sub-bullet):

Using file as User1OEM

1. 3D PDF – DRM001.pdf
 - a. 3D model loaded correctly, then Adobe applied an update (30 September 2021), putting the tester's Elastic Computing 2 (EC2) at version 2021.007.20099, at which point the tester could not open the document any longer.
 - b. Tester was able to open a version of the 3D PDF document, which was not encrypted by Fasoo.
 - c. Tester then deleted the encrypted version and applied the Fasoo encryption to a new copy of the 3D PDF document. Tester was still unable to open the 3D PDF document.
 - i. Whatever update Adobe applied on 30 September 2021) prevented the tester from being able to open a Fasoo encrypted 3D PDF file.
 - d. After decrypting the document, tester was able to open the 3D PDF.
 - e. Later testing (see 1.1.A.6.1) determined that only the 64-bit version of Adobe Reader software was affected by the update Adobe applied. The 32-bit version of Adobe Reader software continued to perform correctly; later testing used the 32-bit version of Adobe Reader software successfully with PDF file types, both 3D model PDF files and non-3D PDF files.
2. PDF – Solicitation.pdf
 - a. Same issue with this non-3D PDF. After the Adobe update was applied, tester could no longer open a Fasoo encrypted PDF.
 - b. Later testing (see 1.1.A.6.1) determined that only the 64-bit version of Adobe Reader software was affected by the update Adobe applied. The 32-bit version of Adobe Reader software continued to perform correctly; later testing used the 32-bit version of Adobe Reader software successfully with PDF file types, both 3D model PDF files and non-3D PDF files.
3. DOCX – Air_Drop_Platform_Rigging_Manual.docx
 - a. Proprietary
 - i. Correctly had full control of the document.
 - b. Official use
 - i. Correctly had full control of the document.
 - c. Confidential
 - i. Correctly had full control of the document.
4. XLSX – Link_Assembly_Bill_Of_Material.xlsx
 - a. Proprietary
 - i. When opening file as User1OEM, Excel indicated that there were errors in the file and fixed them.
 - ii. The first time tester made a change and tried to save, Excel asked if tester wanted to overwrite the current file.

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

- b. Official use
 - i. Correctly had full control of the document
- c. Confidential
 - i. Correctly had full control of the document
- 5. PPTX - Sample_Acceptable_3D_TDP.pptx
 - a. Proprietary
 - i. Correctly had full control of the document
 - b. Official use
 - i. Correctly had full control of the document
 - c. Confidential
 - i. Correctly had full control of the document
- 6. CAD File for Testing - linkSidePlate.STEP
 - a. Proprietary
 - i. Correctly had full control of the document
 - ii. Opened using Notepad without issue
 - b. Official use
 - i. Correctly had full control of the document
 - ii. Opened using Notepad without issue
 - c. Confidential
 - i. Correctly had full control of the document
 - ii. Opened using Notepad without issue

Notes

- 1. Applying document classes
 - a. Tester was able to select all the files and manually apply the document classes.
 - b. However, the software required the tester to re-select the document class for each file; the tester could not simply select "Proprietary" and have it applied to all of the files selected.
- 2. Ownership
 - a. Even though the tester created a MS Word document, once the tester applied the policies he was locked out. For example, applying Confidential policy removed all of the tester's permissions from the document such that he could only View the document – nothing else.
 - b.
 - d. Assigning a document class to a document makes User1OEM the Fasoo Owner of the document. Providing full control for the User1OEM (the user who encrypts a file) becomes designated as the owner of that file.
- 3. Document metadata. When encrypting the files, the following document metadata is removed:
 - a. Description – Title, subject, tags, categories, comments
 - b. Origin – Authors, last saved by, revision number, version number, program name, company, manager
 - c. Content – Content status, language
- 4. Deleting user
 - a. Deleting a user that was created in the Fasoo Admin console and was used to assign a policy cannot be undone. Files encrypted by the deleted user cannot be decrypted.

5.

Using file as User1DLA

- 1. 3D PDF – DRM001.pdf
 - a. 3D model requires using 32-bit version of Adobe Reader software (see 1.1.A.6.1, section about file DRM001.pdf)
 - b. 3D model did not open correctly when using updated 64-bit version of Adobe Reader software.
- 2. PDF – Solicitation.pdf

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

- a. Requires using 32-bit version of Adobe Reader software (see 1.1.A.6.1, section about file Solicitation.pdf)
 - b. Did not open correctly when using updated 64-bit version of Adobe Reader software.
3. DOCX – Air_Drop_Platform_Rigging_Manual.docx
 - a. Proprietary
 - i. Printing with watermark not included
 - b. Official use
 - i. Correct - Permissions restricted to that of an DLA user
 - c. Confidential
 - i. Correct - Permissions restricted to that of an DLA user
4. XLSX – Link_Assembly_Bill_Of_Material.xlsx
 - a. Proprietary
 - i. Printing with watermark not included
 - b. Official use
 - i. Correct - Permissions restricted to that of an DLA user
 - c. Confidential
 - i. Correct - Permissions restricted to that of an DLA user
5. PPTX - Sample_Acceptable_3D_TDP.pptx
 - a. Proprietary
 - i. Printing with watermark not included
 - b. Official use
 - i. Correct - Permissions restricted to that of an DLA user
 - c. Confidential
 - i. Correct - Permissions restricted to that of an DLA user
6. CAD File for Testing - linkSidePlate.STEP
 - a. Proprietary NX
 - i. Printing with watermark not included
 - ii. Opened in Notepad
 - b. Official Use NX
 - i. Correct - Permissions restricted to that of an DLA user
 - ii. Opened in Notepad
 - c. Confidential NX
 - i. Correct - Permissions restricted to that of an DLA user
 - ii. Opened in Notepad

1.1.A.7.2 Test using the browser for each file.

The Fasoo FED product does not implement browser based functionality.

1.1.A.8 Zip file—Apply Policy Set 1 to the contents of the TDP after it is compressed into a ZIP file; verify the policy set functions as expected.

1.1.A.8.1 Access via WinZip.

Software does not support WinZip or 7-Zip, according to its current FED_App_Compatibility spreadsheet. While the software may not support zip compression software at this time, to the level of integration the way the software supports Microsoft Office software, testing found that 7-Zip can be used to compress encrypted files, which can be expanded, and which must be expanded before being accessed or used.

Obtaining WinZip software was not pursued since a process for using 7-Zip was demonstrated.

1.1.A.8.2 Access via 7-Zip.

Chuck – Complete)

Software does not support WinZip or 7-Zip, according to its current FED_App_Compatibility spreadsheet (see 1.1.A.8.1 for workaround).

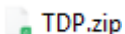
Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

Used 7-Zip to compress the TDP files into a single .Zip file.

30. Assigned the zip file the Proprietary Document class

31. The file's document icon changed to:



32. Could not open the file using 7-Zip – file format not recognized

33. Could not open using Windows Explorer – file format not recognized

34. With Policy Set 1, the recipient would not have permission to decrypt file TDP.zip to try to decompress it.

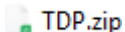
1.1.A.8.3 Access via Windows Explorer.

Software does not support WinZip or 7-Zip, according to its current FED_App_Compatibility spreadsheet (see 1.1.A.8.1 for workaround).

Used Windows to compress the TDP files into a single .Zip file

35. Assigned the zip file the Proprietary Document class

36. The file's document icon changed to:



37. Could not open the file using Windows Explorer – file format not recognized.

38. Could not open using 7-Zip – file format not recognized.

39. With Policy Set 1, the recipient would have not permission to decrypt file TDP.zip to try to decompress it.

1.1.A.9 Apply each restrictive policy by itself to the TDP, one at a time; then verify that the policy functions as described.

1.1.A.9.1 Access via WinZip.

Software does not support WinZip or 7-Zip, according to its current FED_App_Compatibility spreadsheet (see 1.1.A.8.1 for workaround).

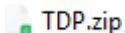
1.1.A.9.2 Access via 7-Zip.

Software does not support WinZip or 7-Zip, according to its current FED_App_Compatibility spreadsheet (see 1.1.A.8.1 for workaround).

Used 7-Zip to compress the TDP files into a single .Zip file.

40. Assigned the zip file the Proprietary Document class.

41. The file's document icon changed to:



42. Could not open the file using 7-Zip – file format not recognized

43. Could not open using Windows Explorer – file format not recognized

44. With Policy Set 2, the recipient would have permission to decrypt file TDP.zip which could then be decompressed as an ordinary unprotected file.

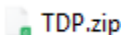
1.1.A.9.3 Access via Windows Explorer.

Software does not support WinZip or 7-Zip, according to its current FED_App_Compatibility spreadsheet (see 1.1.A.8.1 for workaround).

Used Windows to compress the TDP files into a single .Zip file.

45. Assigned the zip file the Proprietary Document class.

46. The file's document icon changed to:



47. Could not open the file using Windows Explorer – file format not recognized.

48. Could not open using 7-Zip – file format not recognized.

49. With Policy Set 2, the recipient would have permission to decrypt file TDP.zip which could then be decompressed as an ordinary unprotected file.

1.1.A.10 As an *unauthorized* user, attempt to manipulate the TDP for Policy Set 1 and Policy Set 2.

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

1.1.A.10.1 Unauthorized users should not have any access permissions.

Works as it is supposed to. DLA users have full rights and OEM users have read only. Could not open files as a logged-out user.

As a DLA user, tester made a copy of and changes to Air Drop Platform Rigging Manual.docx and made it a proprietary document. As an OEM user, tester could view and edit the document.

With the 3D PDF file type, an unauthorized user receives an 'Access denied' error message and is shown only a blank image and cannot open the file.

1.1.A.11 Evaluate how a copy of a DRM-protected TDP continues to be protected.

1.1.A.11.1 Make a copy of the (unchanged) TDP and send it to another person. Does the copy maintain the same level of DRM protections as the original?

As User4DLA, the tester encrypted the Air_Drop_Platform_Rigging_Manual.docx document using Confidential.

DLA users have full rights and OEM users have read only for confidential documents. Tester sent the copy to both his or her LMI email and personal email address and could not access the TDP.

Tester copied the TDP as an OEM user and could not access the Adobe PDF and Word Doc as another OEM user. Tester could open it as another DLA user.

With the 3D PDF file type, an unauthorized user gets an 'Access denied' error message, is shown a blank image, and cannot open the file.

1.1.A.11.2 Make a copy of the (unchanged) TDP and send it to another person. Does the copy maintain the same level of DRM protections as the original?

As User4OEM2, the tester created a document, protected it using the confidential policy, and then followed up with logging in as a DLA employee and looking at the document.

Logged out as an unauthorized user and could not access the document.

1.1.A.12 Evaluate whether DRM protection of a TDP interferes with the routine maintenance process of making backup copies of files.⁴

This can be accomplished by:

1. Applying encryption using Fasoo on the EC2
2. Downloading the file to your local machine.
3. Uploading the file to SharePoint.
4. Downloading the file from SharePoint
5. Performing the test:
 - On local LMI laptop computer, tester made a folder named Testing-Backup
 - As user7 on EC2 Server C, while not logged into Fasoo software, tester accessed folder Test-Data-encrypt on Desktop, which contains encrypted copies of seven test files, then used right-click and copy function to copy all seven files in that folder
 - On local LMI laptop computer, tester used right-click and paste function to put all seven encrypted test files into folder Testing-Backup
 - Folders under OneDrive – Logistics Management Institute (LMI) are backed up regularly during the day, automatically
 - The encrypted files in folder Testing-Backup raised no exceptions or errors from OneDrive in 24 hours
 - One day later, the files in folder Testing-Backup were compared to copies of those files in another folder (a folder not associated with OneDrive) and all seven files in folder Testing-Backup matched their corresponding files in the other folder.

Note: Unable to access OneDrive or SharePoint or other non-local file store from the EC2.

1.1.A.13 Evaluate whether DRM protection of a TDP is compatible with OneDrive or SharePoint or other non-local file store approaches.

⁴ These tests specifically refer to the backup process that many companies run in the background in the case of storage failure.

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

This can be accomplished by:

1. Applying encryption using Fasoo on the EC2
2. Downloading the file to your local machine.
3. Uploading the file to SharePoint.
4. Downloading the file from SharePoint
5. Performing the test:
 - As user7 on EC2 Server C, while not logged into Fasoo software, tester copied seven files of test data into a folder on Desktop of EC2. None of the seven files were encrypted automatically upon being copied onto the EC2. After logging in to Fasoo software as user User2DLA, tester encrypted each file as a Confidential Document class file.
 - Note: for all seven files, only the "Create secured document" option was available; the option to "Create secured document NX" was not available.
 - Next, tester copied seven encrypted files onto local laptop computer, then uploaded those seven encrypted files from local laptop computer into a folder named "Test-Data-Encrypted" under folder Testing on the SharePoint site for DRM.
 - Next, downloaded those seven files from SharePoint into a different folder on local laptop computer, then copied the seven files from that folder on local laptop computer onto Desktop of EC2. Finally, tester decrypted the seven files that came from SharePoint. All files were decrypted.
 - Tester logged out from Fasoo software. Afterwards, all seven files could be read by their native application software.

Note: Unable to access OneDrive or SharePoint or other non-local file store from the EC2.

1.1.A.14 Evaluate revocation.

1.1.A.14.1 Explore the ability for the software to remove permissions once users have the TDP in their possession.

Method and Results

1. On EC2 A
 - a. As User1DLA, tester applied Proprietary to Link_Assembly_Bill_Of_Material.xlsx
2. Copied the file to EC2 C
 - a. On EC2 C, tester logged in as User1OEM
 - b. Tester was able to open the file.
3. On EC2 A
 - a. There was no way to remove individual permissions.
 - b. Tester changed the document class to Confidential.
4. On EC2 C
 - a. Tester waited five minutes. The document class did not change.
 - b. Tester used "Update Policy" to refresh the policy on the EC2.
 - c. The document class for the file did not update.
5. On EC2 A
 - a. Tester revoked permissions (Right-Click > Fasoo > Revoke)
6. On EC2 C
 - a. User1OEM no longer had access to the file.

Conclusion(s)

- The only way to remove permissions remotely is to revoke ALL permissions from the file.
- The "Change class" policy shown in Table in section A.1.7 did not function the way we expected it would.
- Possible workaround: create multiple copies of the same file and designate the different copies to be different Document Classes. That way, all access to one of the copies could be removed while selected users could be given access to an alternative copy in a different Document Class.

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

1.1.A.14.2 Apply permissions, then revoke them one at a time—testing to ensure the permissions were removed.

Based on A14.1, there is no way to remove individual permissions. You can only remove ALL permissions from a file or change the set of policies applied to it (i.e., change the document class assigned to the file).

1.1.A.14.3 What are the limitations for this functionality?

- The major limitation is the lack of ability to remove individual permissions. You can only remove ALL permissions.
- Once the Revoke command has been used, it is no longer possible to use the "" command to request permissions to the file. A new file must be sent.

1.1.A.15 Revocation using an expiration date.

1.1.A.15.1 Test for revocation but use a timeout period after which the permissions are automatically removed.

- EC2 A, as User1DLA, tester applied Confidential document class to Link_Assembly_Bill_Of_Material.xlsx.
- EC2 C, as User1OEM, tester copied the file to EC2 C.
 - Able to open file without issue, which worked as expected.
- Setting a time-based revocation must be performed at the Permissions Setting level (Permissions Policy > Permission Policy).
 - Set rule #7 (OEM – Company Owned) to expire on 6 October 2021 at 11:50 a.m. Pacific Standard Time.
 - After the allotted time, User1OEM's access to the file was automatically revoked.
- After resetting rule #7 back to its original configuration, User1OEM was once again able to open the file.

1.1.A.16 Ensure TDP destruction.

1.1.A.16.1 Explore the possibilities in the DRM software to verify that data has been destroyed.

The software does not provide the capability to destroy a file. The closest the software comes to file destruction is the Revoke functionality, which removes everyone's privileges from the file.

1.1.A.17 Evaluate distribution.

1.1.A.17.1 Can DLA control distribution of the TDP by preventing or providing distribution permissions to a potential supplier?

All permissions originate from DLA. DLA can control distribution by only allowing certain suppliers to create a Fasoo account. Only those potential suppliers with an account may open an EDRM-protected file.

1.1.A.17.2 Evaluate whether the DRM software can prevent potential suppliers from redistributing the TDP without permission from DLA.

While the software cannot prevent the potential supplier from sending the DRM-protected file to someone else, the person receiving the file will not be able to open the file without:

1. A Fasoo account
2. The Fasoo client software installed.

1.1.A.17.3 If the potential supplier attempts to redistribute the TDP without DLA permission, is DLA notified?

No, DLA is not notified. An action against the DRM-protected file is only logged when the person manipulating the file has the Fasoo client software installed and/or is logged into the client software with a valid account.

1.1.A.18 Ensure TDPs provided without DRM protections are accessible (i.e., the DRM client software does not automatically apply permissions).

Files created without DRM protections are accessible by other users without the DRM client software installed. However, if the policies are set up to automatically encrypt particular file extensions, then the files

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.1: Verify DRM Policies Function as Described

will be automatically encrypted and would not be accessible by those without the client software. These files would first need to be decrypted prior to being sent to someone without the client software.

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.2: Evaluate Advertisement Options

Overview:	Evaluate the options DLA has for advertising the TDP while secured by DRM.
Requirements:	R1
Preconditions:	1. A TDP is available for DLA to advertise a new procurement opportunity to an intended group of suppliers. 2. Authorized and unauthorized user sets exist.
Postconditions:	• The procurement opportunity is advertised by DLA to suppliers. • Authorized suppliers can review the advertised procurement opportunity. Unauthorized suppliers cannot review the contents of the advertised procurement opportunity.
Assumptions:	1. Lightweight Directory Access Protocol (LDAP) is configured with authorized users. 2. A way to communicate with a group of authorized supplier users exists through the vendor platform or some external source, such as email or a web portal.

Permutations

1.2.A Evaluate the options DLA has for advertising the TDP while secured by DRM.
1.2.A.1 Evaluate the options for DLA to advertise the procurement opportunity. The minimal options follow:
1.2.A.1.1 Email While Fasoo does not natively support advertising the procurement opportunity represented by a TDP, data protected under the Fasoo DRM can be shared externally to the system via email. In this way, an advertisement method could indirectly share TDP with suppliers. EDRM is primarily intended to protect data rather than facilitate the advertisement of opportunities related to that protected data (i.e., having built-in advertisement method is not an expected feature of an EDRM product). 1.2.A.1.2 Listing on a website Because data protected under Fasoo DRM can be shared externally, it can also be stored in a platform independent of Fasoo and then listed/advertised. TDP listed on a platform independent of Fasoo in such a way would not be viewable until downloaded and decrypted with a local Fasoo client software.
1.2.A.2 Explore the software to evaluate whether it offers additional options for advertising the procurement opportunity.
While Fasoo's FED product does not natively provide a way to send and/or list TDP for the purpose of advertising to a supplier, Fasoo's FED product does support external ways to send and/or list protected data, such as e-mail or posting on a web site. The term "natively" is used to indicate that Fasoo's FED product does not provide an intrinsic, built-in way to send and/or list protected data. EDRM is primarily intended to protect data rather than facilitate the sending and/or posting of protected data. In other words, having built-in transmission and/or distribution method is not an expected feature of an EDRM product.
1.2.A.3 Explore the options for DLA personnel to delay applying DRM to data (e.g., bid packages) until after the final approval steps for the data to be advertised.
There are two ways the DLA can delay applying DRM permissions until the final approval steps: 1. The folder where the TDP will be advertised can be set to encrypt files with specific file extensions when the files are added. 2. Just prior to placing the TDP within the advertising location, DLA could use the manual encryption method to apply DRM permissions.

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.2: Evaluate Advertisement Options

1.2.A.4 Evaluate the ability for authorized non-DLA users to receive data from DLA securely.

Encrypting the TDP prior to it leaving DLA's network will ensure that the data is protected. Fasoo does not provide any intrinsic, built-in way of transporting data –it relies on well-known delivery methods provided by other products instead, such as email, listing on webpage/cloud storage/etc., File Transfer Protocol and Security File Transfer Protocol (FTP/SFTP), etc.

EDRM is primarily intended to protect data rather than facilitate the transport of protected data. That is, having built-in transport method is not an expected feature of an EDRM product.

1.2.A.4 Evaluate the ability for authorized non-DLA users to receive data from DLA securely.

See 1.2.A.4 (above).

1.2.A.5 Evaluate whether a group of authorized supplier users can participate in the procurement opportunity described by a TDP under DRM after DLA has advertised the procurement opportunity through the DRM software solution or an external process.

The authorized group of supplier users would need the following to participate:

1. Fasoo user account
2. Client software installed on their device (Windows/Mac)
3. Active internet connection to receive the file and for the Fasoo FED client software to validate permissions.
 - a. Depending on the permissions, the supplier-user may need to maintain an active connection the entire time they are reviewing the data.

1.2.A.6 Evaluate the ability of the software to allow DLA to confirm receipt of the procurement opportunity advertisement to the intended users.

The Fasoo FED product does not provide an explicit "confirm receipt" functionality. Its admin console logs the activity users perform against a protected file. DLA could dig through the logs to confirm receipt.

1.2.A.7 Evaluate the ability for security policies and DRM controls to travel with the data successfully.

The DRM controls remain with the data unless an authorized action is taken to remove the controls.

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.3: Transfer Data to Many Users Securely

Overview:	50. DLA can transfer data to many users securely, with data protected by DRM. 51. Data must arrive intact and remain intact. 52. DRM protection offers security in transit, thwarting interception (data in transit). 53. DLA can apply access permissions to the data.
Requirements:	R2.1, R2.3, R2.4, R3.1
Preconditions:	The TDP has a policy set applied.
Postconditions:	The TDP has been transferred to two or more users with its policy set intact.
Assumptions:	None

Permutations

1.3.A DLA can transfer data to many users securely, with data protected by DRM. Data must arrive intact and remain intact.
1.3.A.1 Evaluate whether DLA can transfer data to many users securely, with data protected by DRM.
1.3.A.1.1 Evaluate all DRM policy sets per Section A.1.8. The policy sets in Section A.1.8 can be applied to data and then distributed to many users with the same confidence as being delivered to a single user. This is no difference between the two scenarios. While Fasoo does not natively support advertising the procurement opportunity represented by a TDP, data protected under the Fasoo DRM can be shared externally to the system via email. In this way, an advertisement method could indirectly share TDP with suppliers. 1.3.A.1.2 Email the TDP to several users and ask them to manipulate the TDP in a manner that should be denied by Policy Set 1. This test case is satisfied by the results for Test Case Set 1.2 – A11.

1.3.A.2 Evaluate each file in the TDP and confirm that the file received by the supplier is an exact copy of the DLA source file to an acceptable confidence level maintaining that data remains intact.^a
The Fasoo FED tool itself does not provide a way to confirm that the file received by the supplier is the same file that was sent by the DLA. This evaluation will only make use of a single file as a proof of concept. Evaluating each file individually would not provide any additional insight and is therefore not necessary to evaluate this test case. - As User1DLA, tester encrypted the Air_Drop_Platform_Rigging_Manual.docx file using the Confidential document class. - Checksum SHA256: A12101131EBCBC6059753413A1BE527F9785D9CC6A201AA74E65097FEA03737E - Tester emailed the encrypted document to his or her LMI email account. - Tester downloaded the attachment to a local machine. - Tester created a new email and sent the encrypted document back to the EC2. - As User1OEM, tester downloaded the encrypted file. - Tester performed a checksum of the encrypted file and received the following result: - SHA256: 6C1337B21139F55FC4A7B59ABD07B180973FDDA695ED0828C3E6F199121F8CAF - The checksums do not match. - Conclusion - Changes occur to a file when it is sent via email, most likely to the file's metadata. - It does not appear that testers can use checksum to validate that the file DLA sends is the file the supplier receives. Notes about checksum: Used Z-zip to create a checksum for Air_Drop_Platform_Rigging_Manual.docx. Before encryption: SHA256: E60B9586B9EC0E7DE1BC2C737BB3C564DAEAA2235483C62F9C3C61DFE228B047 After encryption: SHA256: F7C3016393F6EAD005B2AE3A80DADAF982082CA501150A2224BC40408B04996

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.3: Transfer Data to Many Users Securely

After decryption:

SHA256: 69ABBA08FB287A9A73E319A70DDF258C8D2AD39A9749F4E7939019153908D9A3

The checksum changes from that of the original after encryption and decryption.

Used Z-zip to create a checksum for Sample_Acceptable_3D_TDP.pptx.

Before encryption:

SHA256: 99B7096686CEE0A65C08A255F45DBA3916284C67E285D240070936AF106B5FC2

After encryption:

SHA256: 1EF33AE27105E7C45F6927EF21A98C302D60564D2653D245161601F7569EA3AB

After decryption:

SHA256: 266BF98F70B1542B808D2C0D5DA51E85ECEE66C159926B3BF94B43F41347287

Conclusion

When the file is encrypted and then decrypted, changes occur that alter the file itself. The changes to the file result in different checksums.

1.3.A.3 Evaluate features of the DRM software to prevent or detect unauthorized changes after the file is received.

To prevent unauthorized access:

1. The file itself is encrypted.
2. The recipient must have the client software installed in order to access the file.
3. The recipient must have an active Fasoo account in order to access the file.

To detect unauthorized changes:

1. Changes can only be detected if the recipient has the client software installed.
2. Attempts to make unauthorized changes are logged by the client software (sent to the central policy server).
3. If client software is not installed, attempts to make unauthorized changes are not logged and therefore will not be detected.

1.3.A.4 Evaluate whether DRM protection offers security in transit, thwarting interception (data in transit).

1.3.A.4.1 Use software, such as Wireshark (<https://www.wireshark.org/>), to simulate a man-in-the-middle attack. Review this write up for a possible approach: <http://worldcomp-proceedings.com/proc/p2011/SAM4991.pdf>

Fasoo does not offer any intrinsic, built-in encrypted VPN data transfer method (which was expected).

EDRM is primarily intended to protect data rather than facilitate the transport of protected data; having built-in transport method is not an expected feature of an EDRM product.

The Fasoo FED tool relies on the encryption placed on the file to protect data during transit. If the data is intercepted during transit, the bad actor must get through the encryption before accessing the file.

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.4: Assign Access Permissions to DLA and Non-DLA Users

Overview:	Explore the ability to assign access permissions (policy sets) to groups of non-DLA users for the TDP. Grouping suppliers and then giving them DRM permissions to a TDP would enable DLA to manage access better. DLA can apply unique access permissions by user.
Requirements:	R0.2, R3.3, R5.3, R21
Preconditions:	The non-DLA users are not listed in our LDAP.
Postconditions:	Ideally, the non-DLA users can be assigned specific policy sets but this precondition is yet to be determined.
Assumptions:	The software can assign policy sets to groups of users for a TDP.

Permutations

1.4.A Explore assigning different access permissions to sets of non-DLA users—these users are not listed in LDAP.

1.4.A.1 Evaluate whether it's possible to govern access to TDP using a large group of users. For example, User Group A has Policy Set 1 for the TDP while User Group B has Policy Set 2 for the TDP.

It is possible to govern access to TDP using a large group of users. During the prototype, we created two groups of users. One group was assigned Policy Set 1 permissions to data and the other was assigned Policy Set 2 permissions to data. Each of the groups could be assigned a large number⁵ of users.

1.4.A.2 Show that different permissions can be assigned to different groups.

1.4.A.2.1 Test using each file's native application (with the local agent active).

This was the foundation of the prototype (see 1.4.A.1). The test was performed in Test Case Set 1.1 Actions 1.4.A.6 and 1.4.A.7.

1.4.A.2.2 Test by accessing the TDP via the browser.

The Fasoo FED product does not implement browser-based functionality.

1.4.A.3 Explore the possibility of assigning permissions to roles—then assigning those roles to different user groups.

1.4.A.3.1 Can we assign roles to groups of Non-DLA users? Show that roles with different permissions can be assigned to different groups.

The system provides the ability to create roles and titles but does not allow those roles and/or titles to be targeted with its own set of permission. The permissions are handled at the group and/or individual user level.

1.4.A.3.2 Test using each file's native application (with the local agent active).

The test was performed in Test Set 1.1 1.4.A.6 and 1.4.A.7.

1.4.A.3.3 Test by accessing the TDP via the browser.

The Fasoo FED product does not implement browser-based functionality.

1.4.B Explore assigning complete access to DLA personnel for DLA-originated data.⁶

1.4.B.1 Explore whether different permissions and access levels are needed to administer DRM policies or access reports produced by DRM software—a small group of DLA personnel might need different access levels to control administration of DRM.

Administrative users can be created with different levels of access within the system.

⁵ Fasoo stated that they have more than 700,000 users at Samsung. Here, the tester considers “large” to mean at least 700,000 users.

⁶ To reduce the overall disruption to DLA processes, it is recommended that DRM permissions be assigned even to documents behind DLA's firewall. For example, what if a product data specialist at DLA puts a file in the data store where the public can access

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.4: Assign Access Permissions to DLA and Non-DLA Users

1.4.B.2 Explore whether DLA personnel could place data in the DLA data store without using local agent software.

DRM permissions cannot be added to the data without the local agent software. However, DLA can place data in their own data store using whatever method they would like. But the permissions assigned to the data must use the local agent software.

1.4.B.3 Explore whether DLA personnel could access data of other DLA personnel in the DLA data store without restrictions and without using local agent software.

DLA personnel need the local agent software in order to access DRM-protected data.

1.4.C Explore obtaining permission to access the TDP if not initially given access permissions:

1. Attempt to access a file as a user without access permission.
2. Use functionality built into the DRM software to request permission to access the TDP.
3. Grant access as an administrator.
4. Access the TDP in the limits of the granted privileges.

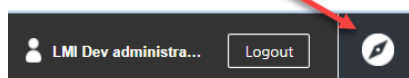
1.4.C.1 Test using each file's native application (with the local agent active).

Note: We're only testing one Excel file instead of all of the file types. The purpose is to test the functionality itself, not that it works against all file types.

1. As User1DLA, tester encrypted the Excel file as confidential.
2. Tester logged in as User1OEM and used the Provisional Permission Request to request Edit permissions for the file.
3. On local machine, tester logged in to the admin console and approved the request.
4. The User1OEM was not notified when the additional privileges were given.
5. After edit privileges were approved, User1OEM was able to edit the Excel file.

Notes:

- When making a request, the software uploads the document, sending it to the policy server. When permissions are granted, the policy server sends it back to the user's machine with the altered permissions set.
- The approval location for these requests is found in the upper right-hand corner of the admin console. The location and usage of the functionality is not explained in the admin guide.



- The request did not show up under the pending requests screen. The tester had to drill down into the individual groups under Logs to find the request in order to approve it. This would require extra work on the part of the DLA admin. The approval showed up on the "complete" listing.

1.4.C.2 Test by accessing the TDP via the browser.

The Fasoo FED product does not implement browser-based functionality.

1.4.D Explore DLA's ability to deny permission to access the TDP.

1.4.D.1 The previous tests assume permission is granted when requested. How does the software allow DLA to deny a user's request for access?

Note: We are only testing one Excel file instead of all of the file types. The purpose is to test the functionality itself, not that it works against all file types.

it (with DRM permissions), then a potential bidder sends an email to someone at DLA, such as a product specialist (PS), with a question about the data. The normal DLA workflow would allow the other person at DLA, the PS, to grab a copy from the same data store where the supplier got it to respond to the question. The workflow would change if DRM permissions intruded on that process.

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.4: Assign Access Permissions to DLA and Non-DLA Users

1. As User1DLA, tester encrypted the Excel file as confidential.
2. Tester logged in as User1OEM and used the Provisional Permission Request to request Print with Watermark permissions for the file.
3. On local machine, tester logged in to the admin console and rejected the request.
4. The User1OEM was not notified that the request was rejected.
 - a. This would require the user to keep checking to see if they have access and/or contact their DLA point of contact (POC).

Task 1: Transfer Data to Many Users Securely

Test Case Set 1.5: Policy Automation

Overview:	Explore the system's ability to automatically apply policy sets based on applicable factors. The factors are limited to those allowed by the software.
Requirements:	R26
Preconditions:	The TDP does not have any policies applied, i.e., it's a clean slate.
Postconditions:	The TDP takes on the applicable policies once the trigger criteria for the automation is met.
Assumptions:	Data can remain in current repositories (R20).

Permutations

1.5.A Establish the factors that the software allows for automating the application of a policy set. For example, can the system revoke privileges automatically 30 days after TDP publication?

See Test Case Set 1.1 1.5.A.3. There are several ways in which the software can automatically apply DRM policies.

1.5.B Establish automation for three to five of the most likely scenarios and test the capability.

- Policy automation where files automatically encrypted by file extension when the file is initially created by the native application:
 - When policy is set up to encrypt .docx files, and when logged in to Fasoo software as user ID Imidev1, tester created a new .docx file, which was encrypted automatically.
 - While newly created .pptx and .xlsx files were not encrypted automatically, policy was not set up to encrypt those file extensions automatically.
- Policy automation where files automatically encrypted when document is loaded:
 - When policy is set up to encrypt .stl files, a .stl file copied onto a PC was encrypted automatically, even when not logged in to Fasoo software.
- Policy automation where files automatically encrypted when placed in a folder targeted to encrypt files with specific file extensions as soon as they are added:
 - When policy is set up to encrypt files placed in a specific folder, file with specific file extension was encrypted when it was added, even when not logged in to Fasoo software.

Task 2: Transfer Data Securely in Reverse

Test Case Set 2.1: Transfer Data Securely in Reverse

Overview:	The supplier transfers TDP data to DLA. DLA receives and ingests the data into its systems. DRM security is maintained throughout the process. Data must arrive intact. These tests serve as a continuation of the work from Task 1 and focus on ensuring a baseline in the performance and maturity of the DRM software when data flows in the reverse direction.
Requirements:	R9.1, R9.3, R11, R12, R13, R14, R24
Preconditions:	1. Task 1: Data can be transferred to many users securely. 2. An appropriate policy set is applied to data; authorized and unauthorized user sets exist.
Postconditions:	TDPs arrive at DLA within DRM policy controls and DLA can ingest the data.
Assumptions:	1. A collection of authorized users exists representing supplier users and the central DLA authority. 2. The same level of DRM is applied to data after modification by authorized supplier users.

Permutations

2.1.A Evaluate the ability of the DRM software to transfer and receive data in the TDP in the reverse direction.
2.1.A.1 Evaluate the supplier's ability to securely send TDP to DLA.
See Test Case Set 1.2 2.1.A.4. The supplier uses the local client software to apply policies in the same manner as DLA and would rely on the encryption to protect the TDP. Once the file is encrypted with DRM protections, the supplier would use transport methods outside of the software to send data to DLA (e.g., email, SFTP, etc.). EDRM is primarily intended to protect data rather than facilitate the transport of the protected data. That is, having built-in transport method is not an expected feature of an EDRM product.
2.1.A.2 Evaluated the ability of DLA to receive various forms of TDPs (unchanged to brand new) with DRM protection.
See Test Case Set 1.2 2.1.A.4. DLA can receive EDRM-protected files using transport methods outside of the EDRM software, at which point the EDRM client determines the permissions a DLA employee possesses relative to the file.
2.1.B Evaluate each file in the TDP and confirm that the file received by DLA is an exact copy of the file sent by the supplier to an acceptable confidence level.
Set Test Case Set 1.3 2.1.A.2. The software does not provide a way to confirm that the file received by DLA is the same file that was sent by the supplier.
2.1.C Evaluate the ability of the DRM software to transfer and receive data in the TDP in the reverse direction.
2.1.C.1 Policy Set 1
2.1.C.1.1 TDP data has experienced no changes. The file will arrive at DLA with the same permissions DLA originally applied, as long as the supplier did not manually remove the DRM protections. With Policy Set 1, the supplier would have "view only" permission, and would not be able manually to remove permissions DLA originally applied. 2.1.C.1.2 TDP data has experienced no changes, but the TDP now includes authorized additional data (e.g., adding a change request form). Yes for existing files (see 2.1.C.1.1) and maybe for files newly added. The supplier must manually apply the DRM permissions to the file using the local client software. But it is up to the supplier to apply these permissions. There is no guarantee that the supplier would apply the permissions to the additional data.

Task 2: Transfer Data Securely in Reverse

Test Case Set 2.1: Transfer Data Securely in Reverse

2.1.C.1.3 TDP data initially delivered to the supplier has experienced authorized changes (e.g., a change request form plus changes to one or more files in the envelope).

As long as the supplier has the local client software and edit permissions, the supplier can make authorized changes to files. The files will retain DRM permissions as long as the supplier did not purposely remove the permissions (though DLA is not likely to give suppliers permissions to decrypt the files). With Policy Set 1, the supplier would have “view only” permission, and would not be able manually remove permissions DLA originally applied.

2.1.C.2 Policy Set 2

2.1.C.2.1 TDP data has experienced no changes.

As long as the supplier did not manually remove the DRM protections, the file will arrive at DLA with the same permissions DLA originally applied.

2.1.C.2.2 TDP data has experienced no changes, but the TDP now includes authorized additional data (e.g., adding a change request form).

Yes for existing files (see 2.1.C.2.1) and maybe (for files newly added). The supplier must manually apply the DRM permissions to the file using the local client software. But, it's up to the supplier to apply these permissions. There is no guarantee that the supplier would apply the permissions to the additional data.

2.1.C.2.3 TDP data initially delivered to the supplier has experienced authorized changes (e.g., a change request form plus changes to one or more files in the envelope).

As long as the supplier has the local client software and edit permissions, the supplier can make authorized changes to the files. The files will retain the DRM permissions as long as the supplier did not purposely remove the permissions (though DLA is not likely to give suppliers permissions to decrypt the files).

2.1.D Test using the browser: data transfer in the reverse direction when the TDP data initially delivered to the supplier from DLA.

2.1.D.1 Policy Set 1

2.1.D.1.1 TDP data has experienced no changes.

The Fasoo FED product does not implement browser-based functionality.

2.1.D.1.2 TDP data has experienced no changes, but the TDP now includes authorized additional data (e.g., adding a change request form).

See above.

2.1.D.1.3 TDP data initially delivered to the supplier has experienced authorized changes (e.g., a change request form plus changes to one or more files in the envelope).

See above.

2.1.D.2 Policy Set 2

2.1.D.2.1 TDP data has experienced no changes.

The Fasoo FED product does not implement browser-based functionality.

2.1.D.2.2 TDP data has experienced no changes, but the TDP now includes authorized additional data (e.g., adding a change request form).

See above

2.1.D.2.3 TDP data initially delivered to the supplier has experienced authorized changes (e.g., a change request form plus changes to one or more files in the envelope)

See above.

Task 2: Transfer Data Securely in Reverse

Test Case Set 2.2: Transfer Data Generated by the Supplier in Its Enterprise Securely in Reverse

Overview:	The supplier can initiate or apply DRM policies on new, original-to-the-supplier TDP data.
Requirements:	R13
Preconditions:	1. Task 1: Data can be transferred securely to many users. 2. An appropriate policy set is applied to data; authorized and unauthorized user sets exist.
Postconditions:	The TDP exists within the controls of DRM policy set. DLA did not initiate applying the DRM policy set to data, although DLA assistance may have been needed in applying the DRM policy.
Assumptions:	1. A collection of authorized users exists representing supplier users and the central DLA authority. 2. An appropriate level of DRM can be applied to data created by authorized supplier users.

Permutations

2.2.A Evaluate the ability of the supplier to use DRM software to secure a new, unique-to-the-supplier TDP.

2.2.A.1 Evaluate the supplier's ability to secure data without DLA's input.

See Test Case Set 2.1 2.2.A. The supplier will use the local client software to manually apply the DRM permissions.

2.2.A.2 Evaluated the ability of DLA to receive data under DRM that has never existed at the agency before.

See 2.2.A.1. Once the supplier uses the local client software to manually apply the DRM permissions, they can send the data to DLA. DLA can then use the local client software to access the data.

2.2.B Test using the local agent: when data is transferred in the reverse direction.

2.2.B.1 Policy Set 1

2.2.B.1.1 The TDP is new data, unique to the supplier, and created for the specific procurement (e.g., a new TDP that has never existed in DLA's systems prior).

See 2.2.A.2.

2.2.B.2 Policy Set 2

2.2.B.1.2 The TDP is new data, unique to the supplier, and created for the specific procurement (e.g., a new TDP that has never existed in DLA's systems prior).

See 2.2.A.2.

2.2.C Test using the local agent: when data is transferred in the reverse direction.

2.2.C.1 Policy Set 1

2.2.C.1.1 The TDP is new data, unique to the supplier, and created for the specific procurement (e.g., a new TDP that has never existed in DLA's systems prior).

The Fasoo FED product does not implement browser-based functionality.

2.2.C.2 Policy Set 2

2.2.C.1.2 The TDP is new data, unique to the supplier, and created for the specific procurement (e.g., a new TDP that has never existed in DLA's systems prior).

The Fasoo FED product does not implement browser-based functionality.

Task 3: Transfer Data Securely with Validity Checks

Test Case Set 3.1: Check the Validity of Data Transferred from DLA to the Supplier

Overview:	An exact copy of the data is transferred and remains identical to the source upon arrival, passing the validity check.
Requirements:	R2.2, R4.7
Preconditions:	Task 1: Data is transferred securely from the DLA data store to the supplier.
Postconditions:	The TDP's validity is known to the software or server.
Assumptions:	- For permutations involving native application testing, the supplier has installed the DRM platform's local agent and the local agent app is active. - A collection of authorized users exists representing supplier users and the central DLA authority. - Vendor's DRM policies can be enforced when the native application is used, and local agent app is active. The local agent automatically performs the validity check upon receipt before the supplier performs other actions with the data.

Permutations

3.1.A Evaluate the ability of the DRM software to check the validity of the data in the TDP after it is sent from the DLA data store to the supplier.

3.1.A.1 Evaluate each file in the TDP and confirm the results of the validity checks to an acceptable confidence level.

A supplier user can right-click the file and view the Fasoo permissions to see who applied the DRM policies to the file. This is the only way that the supplier can validate that the file was sent by DLA.

Owner	User1DLA(User1DLA)	Change	Created by	User1DLA
Group	DLA		Group	DLA
Domain code	0100000000002405			

3.1.A.2 Evaluate the ability to share the results of validity check with the intended recipients and originators.

Limited.

- The supplier can send DLA a screen shot of the Fasoo properties on the file.
- DLA can check the logs and see who accessed the file. From there, DLA can surmise that the supplier has the correct file.

3.1.B Local agent testing. Explore how the DRM platform reports on the validity checking of data that the supplier receives in a TDP using native applications (with the local agent active) for their respective file formats (or the container, e.g., .zip).

3.1.B.1 Using a central policy repository server with Policy Set 1 applied, explore the validity checking of newly created and transferred TDP content from the perspective of

3.1.B.1.1 The DLA administrator, i.e., transaction logs, browser console logs.

The Fasoo logs will identify who accessed the file, when, and what actions were taken on the file.

3.1.B.1.2 The supplier, i.e., file hashes, Wireshark logs.

See 3.1.A.1.

Task 3: Transfer Data Securely with Validity Checks

Test Case Set 3.1: Check the Validity of Data Transferred from DLA to the Supplier

3.1.C Browser application testing—Explore how the DRM platform reports on the validity checking of data that the supplier receives in a TDP (or the container, e.g., .zip) using the browser applications (Chrome, etc.).

3.1.C.1 Using a central policy repository server with Policy Set 1 applied, explore the validity checking of newly created and transferred TDP content from the perspective of

3.1.C.1.1 The DLA administrator, i.e., transaction logs, browser console logs.

The Fasoo FED product does not implement browser-based functionality.

3.1.C.1.2 The supplier, i.e., file hashes, Wireshark logs.

See above.

3.1.C.2 Using a central policy repository server with Policy Set 2 applied, explore the validity checking of newly created and transferred TDP content from the perspective of

3.1.C.2.1 The DLA administrator, i.e., transaction logs, browser console logs.

The Fasoo FED product does not implement browser-based functionality.

3.1.C.2.2 The supplier, i.e., file hashes, Wireshark logs.

See above.

Task 4: Transfer Data Securely in Reverse with Validity Checks

Test Case Set 4.1: Check Validity in Reverse

Overview:	To explore: (1) the features for indicating that the file received by the DLA is an exact copy of the file sent by the supplier; (2) features and processes for obtaining validity checks; and (3) features and processes for distributing validity checks, i.e., the visibility of validity checks.
Requirements:	9.2
Preconditions:	Task 2: Data is transferred from the supplier to the DLA data store securely.
Postconditions:	The TDP's validity is known to the software or server; validity check data can be furnished to DLA and available to the supplier.
Assumptions:	Local agent ▪ The supplier has installed the vendor's local agent. ▪ The local agent automatically initiates the validity check upon receipt of data at DLA, before DLA performs any other actions with the data. Browser: The validity check is initiated automatically upon receipt of data at DLA, before DLA performs any other actions with the data.

Permutations

4.1.A Evaluate the ability of the DRM software to check the validity of the data in the TDP.
4.1.A.1 Evaluate each file in the TDP and confirm the results of the validity checks to an acceptable confidence level.
4.1.A.1.1 What validity checks are performed? See Test Case Set 3.1 4.1.A.1. Limited. The system does not perform validity checks automatically. The supplier would need to right-click on the file and view the Fasoo properties. 4.1.A.1.2 How are results of the validity checks (pass or fail) indicated? Limited. It is up to the individual supplier user to right-click and view the Fasoo properties. There is no automatic validity check. 4.1.A.1.3 When or how often are validity checks performed? Limited. Validity checks are a manual process.
4.1.A.2 Evaluate obtaining results of validity checks.
4.1.A.2.1 Does the supplier create validity check data automatically? No. 4.1.A.2.2 Are validity checks (pass or fail) performed automatically? No. 4.1.A.2.3 Does the sender receive validity check results automatically? No. 4.1.A.2.4 Are validity check results transmitted as a separate communication? Not acceptable. See Test Case Set 3.1 4.1.A.2.
4.1.A.3 Evaluate sharing the results of validity checks with both parties, supplier and DLA.
4.1.A.3.1 Are validity check results passed to DLA automatically? No. 4.1.A.3.2 Is action needed to send validity check results to DLA? Yes—though the check result is not acceptable. See Test Case Set 3.1 4.1.A.2. 4.1.A.3.3 Can DLA evaluate validity check results independently? No. DLA would need the supplier to send them a screen shot. See Test Case Set 3.1 4.1.A.2.

Task 4: Transfer Data Securely in Reverse with Validity Checks

Test Case Set 4.1: Check Validity in Reverse

4.1.A.4 Test using the local agent—Policy Set 1 under the following conditions:

4.1.A.4.1 When the TDP has been changed only by adding one or more files (e.g., adding a change request form).

Not acceptable:

1. The validity check available does not change when one or more files are added to the TDP.
2. If the TDP package itself has DRM protections, DLA can check the logs to see if the TDP was edited, but the logs will not indicate that a new file was added.

4.1.A.4.2 When the TDP has been modified.

Limited:

1. The validity check available does not change when the TDP is modified.
2. DLA can check the logs to see if the TDP was modified.

4.1.A.4.3 When an entirely new TDP is created.

Not acceptable. See Test Case Set 3.1 4.1.A.2. The Fasoo properties will list the supplier as the owner of the TDP.

4.1.A.4.4 When the original TDP is used, unchanged, i.e., the supplier did not change the TDP supplied by DLA but is now sending that TDP back to DLA. Can the software check the validity, indicating that the TDP has not been changed?

Limited. DLA can check the logs to see if any edit actions were performed on the TDP.

4.1.A.5 Test using the local agent—Policy Set 2 under the following conditions:

4.1.A.5.1 When the TDP has been changed only by adding one or more files (e.g., adding a change request form). Can the software detect that the TDP now has additional files?

See A.4.1. No. The software cannot detect that new files were added to the TDP.

4.1.A.5.2 When the TDP has been modified.

Same as 4.1.A.4.2.

4.1.A.5.3 When an entirely new TDP is created.

See 4.1.A.4.3.

4.1.A.5.4 When the original TDP is used, unchanged.

See 4.1.A.4.4.

4.1.A.6 Test using the browser—Policy Set 1 under the following conditions:

4.1.A.6.1 When the TDP has been changed only by adding one or more files (e.g., adding a change request form).

The Fasoo FED product does not implement browser-based functionality.

4.1.A.6.2 When the TDP has been modified.

See above.

4.1.A.6.3 When an entirely new TDP is created.

See above. 4.1.A.6.4 When the original TDP is used, unchanged.

See above.

4.1.A.7 Test using the browser—Policy Set 2 under the following conditions:

4.1.A.7.1 When the TDP has been changed only by adding one or more files (e.g., adding a change request form).

The Fasoo FED product does not implement browser-based functionality.

4.1.A.7.2 When the TDP has been modified.

Task 4: Transfer Data Securely in Reverse with Validity Checks

Test Case Set 4.1: Check Validity in Reverse

See above.

4.1.A.7.3 When an entirely new TDP is created.

See above.

4.1.A.7.4 When the original TDP is used, unchanged.

See above.

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.1: Control Access to the TDP

Overview:	A supplier currently only needs a Commercial and Government Entity (CAGE) code to log in and access the TDP on DLA's Internet Bid Board System (DIBBS) website. Explore the ability for DLA to use the software to control who can obtain the data. For example, when DLA posts the TDP on DIBBS for distribution, does the software offer any controls to limit who can obtain the data?
Requirements:	R5.1
Preconditions:	None, this set of test cases explores the capabilities of the DRM software.
Postconditions:	Only authorized user can access the TDP.
Assumptions:	Task 1 has been completed.

Permutations

5.1.A Repository Control

5.1.A.1 Evaluate whether the software can store files with their access governed by the permissions one has in the software.

Fasoo FED does not provide a method for storing files.

5.1.A.2 Evaluate whether the software can govern the access to files in another specified location (e.g., data can remain in its current repositories) by the permissions one has in the software.

Yes. DLA can apply DRM permissions to the files and leave them in their current repositories.

5.1.B Roles

5.1.B.1 Evaluate whether the software can assign roles to non-DLA members.

5.1.B.1.1 Is it possible to loop suppliers into DLA's circle of trust and assign one or more roles to a supplier? This would enable the supplier access to only those TDPs that fall in its purview.

Limited. Permissions cannot be assigned by role; they can only be assigned to a group and/or individual user:

1. At the group level, users may only have one set of permissions.
2. For users that are members of more than one group at the same time, the most restrictive permissions of every group the user is a member of apply.
3. Individual users can have unique permissions, but these permissions would override those of all the groups in which the user is a member.
4. Permissions assigned to an individual user are different from permissions assigned to a user group of one member, where permissions only override other permission when they are more restrictive (see point 2 above).

5.1.B.2 If roles can be assigned to non-DLA members, work with the team to set up a demonstration.

5.1.B.2.1 Can the software control the types of TDP a supplier can access, e.g., radar antennas?

Somewhat. The software can control the types of TDP files the supplier can access by file extension. For example, a user could be locked down such that they can only access text and MS Word files. This method could be used to block mechanical parts manufacturers from accessing Intermediate Data Format (IDF) circuit board files (e.g., .emn, .brd, .bdf, .idb file types).

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.2: Local Agent—Identify Who, When, and Where

Overview:	The TDP can be accessed from a native application using the local agent. These test cases explore the information from the DRM software. Discover the types of information the software can provide, such as the following: ▪ Who accessed or attempted to access the TDP? ▪ Who made changes to or attempted to make changes to the TDP? ▪ When was the TDP accessed or attempted? ▪ When were the changes made or attempted? ▪ Where was the TDP accessed or attempted? ▪ Where were the changes made or attempted? Test cases are evaluated using Policy Set 1 and 2.
Requirements:	R4.3, R4.4, 4.5, 4.6, R6.2, R25
Preconditions:	The TDP is available to be accessed, a policy set is applied to the TDP, and authorized and unauthorized user sets exist.
Postconditions:	The access log is updated showing information for the actions performed on the TDP.
Assumptions:	Tasks 1 and 3 have been completed.

Permutations

5.2.A Explore the ability for DLA to track who receives protected data.
5.2.A.1 When the supplier attempts to access the TDP, does the software send a notification with the identity of the user making the attempt?
Limited: 1. Action log entries are logged when actions are performed against the TDP. 2. The supplier must have the local client software installed. Without the client software, log entries will not be sent, but nor will the supplier have access to the TDP. In other words, the client software must be active for the supplier to gain access to the TDP.
5.2.A.2 If a notification is sent, what kinds of information are provided?
The following information is logged and can be accessed via the admin console: 1. User ID 2. Username 3. Job title code 4. Job title name 5. Group code 6. Group name 7. Date used 8. IP Address 9. OS 10. File name 11. Original file name 12. Content ID 13. Document type a. FED-N 14. Class/system a. Basic NX class b. Confidential c. Official use d. Proprietary 15. Owner name 16. Owner ID

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.2: Local Agent—Identify Who, When, and Where

- 17. Action
 - a. Change class
 - b. Change owner
 - c. Change permission
 - d. Create
 - e. Decrypt
 - f. Edit
 - g. Print without watermark
 - h. Revoke
 - i. View
- 18. Result
 - a. Success
 - b. Fail

5.2.B While the TDP is remote (i.e., located with the supplier), explore the software's ability to do a number of tasks.

5.2.B.1 Determine who attempts to access the TDP.

Limited. A log entry is created when an authorized user attempts to access to the TDP, but only if the client software is installed and has a connection.

Note: having a connection is a prerequisite for even creating a log entry. No indications were observed of a process where a log entry could be created offline then later transmitted after a connection was re-established.

5.2.B.2 Determine who is making the changes.

Limited. A log entry is created when a authorized user attempts to make a change to the TDP, but only if the client software is installed and has a connection.

Note: having a connection appears to be a prerequisite. See 5.2.B.1.

5.2.B.3 Determine who attempted to make changes but was denied by the system.

Limited. A log entry is created when a authorized user attempts to make a change to the TDP, but only if the client software is installed and has a connection.

Note: having a connection appears to be a prerequisite. See 5.2.B.1.

5.2.B.4 Determine when the changes are made.

Limited. A time is associated with the log entry that is created, but only if the client software is installed and has a connection.

Note: having a connection appears to be a prerequisite. See 5.2.B.1.

5.2.B.5 Determine where (geographic location) the changes occur.

No. The software does not have this capability.

5.2.B.6 Determine the application used to access or manipulate the TDP.

No. The software does not have this capability.

5.2.B.7 Determine how often information is sent back to DLA, e.g., is a log entry sent each time a file is saved and when the file is closed?

Yes. A log entry is created each time an action is performed on the document:

1. Change class

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.2: Local Agent—Identify Who, When, and Where

2. Change owner
3. Change permission
4. Create
5. Decrypt
6. Edit
7. Print without watermark
8. Revoke
9. View

5.2.C While the TDP is remote, i.e., located with the supplier, explore the software's ability to do the following:

5.2.C.1 Determine who made the changes.

Yes. The Fasoo username of the person who made the change is included in the log.

5.2.C.2 Determine when the changes were made.

Yes. The log contains time stamps, and each log entry has a time stamp. The time stamp uses the time zone assigned to the policy server.

5.2.C.3 Determine where (geographic location) the changes occurred.

Limited. An IP address is included in the log, and an Internet Protocol (IP) address is part of each log entry. The geographic location can be found by performing a lookup on the IP.

5.2.D When not connected, what does the local agent allow the user to do?

5.2.D.1 Can the local agent authenticate the user when not connected?

Background:

The planned approach for testing offline access functionality was to use a software testing tool to simulate having our test environment, EC2s in an AWS cloud, appear to be disconnected from the Internet, as far as the DRM local client software was concerned. We found that the software tool we intended to use did not have the functionality to disconnect the Fasoo local client software from accessing the Internet, while still maintaining Internet connectivity to support a Remote Desktop Connection to the EC2 for doing our test. Consequently, we employed an alternative method, which is described below.

Method:

We used a separate laptop computer, running Windows 10 operating system, instead of Windows Server 2016 operating system as on the EC2s (using these different versions of Windows operating systems is not expected to affect the functionality of the local client software). The Fasoo local client software was installed on this separate laptop computer and encrypted versions of the test files were copied onto it.

The local client software ran well on Windows 10 operating system, with what appeared to be the same functionality as seen on the EC2s, when connected to the Internet. On the separate laptop computer, the connection to the Internet was disabled to simulate offline operation.

Test environment notes:

- Windows 10 Home x 64
- Notepad.exe
- .txt File format

While logged into the Fasoo desktop client software, after selecting "Online" for Login Status when Internet access is lost, the user is automatically logged out of the desktop client software after a period of one to four minutes. This is likely a polling check on a five -minute interval by the client software to check for an active connection. After the automatic logout, the user cannot log back into the desktop client software again until Internet access is restored.

This behavior is different from the behavior expected of the Fasoo local client software as described in a DRM Introductory Exercises file received from Fasoo. What that file describes in section 2.2.7, Offline

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.2: Local Agent—Identify Who, When, and Where

Access, is that the user should continue to be logged in for longer periods, more than 10 minutes, and should be able to open protected files, although offline access is restricted to “view only” access. The other options for Login Status—“Offline: and “PC Checkout”—were not tested; the Fasoo-supplied DRM Introductory Exercises file does not specify that the user needs to use a particular login option to activate offline access features.

Note: as mentioned in Test Case Set 1.1, Action A4, for this testing, every permission rule created covered all three options for Login Status: Online, Offline, and PC Checkout, as shown in the example in that section.

5.2.D.2 Can the user authenticate while connected, then disconnect and continue working with the files? What are the limitations to what the user can do while disconnected?

See Action 5.2.D.1 for Method.

Test environment notes:

- Windows 10 Home x 64
- Notepad.exe
- .txt File format

While the user is logged out of the Fasoo desktop client software, they receive no access to documents protected under DRM. Attempts to open documents that the user would otherwise have access to fail with a view permission error. Because the desktop client software automatically logs the user out after a brief period of Internet access loss, when the user selects “Online” for Login Status, the user cannot access their Fasoo-protected documents offline on a system with the desktop client software installed.

Some confusion here is caused by the Fasoo documentation referring to “offline” access. There did not seem to be a way to exercise the other options for Login Status—“Offline” and “PC Checkout”—so they were not tested. At this point, since the offline access feature was not performing as the Fasoo documentation described, the tester understands offline access to be external access to a document on a system with an Internet connection, but no Fasoo desktop client software installed (external email sharing).

It is also worth noting that if a document under DRM is open while Internet access is lost, behavior becomes somewhat unpredictable. The user can continue to view the document until the polling event eventually logs them out. The user can also continue to make and save changes until the polling event eventually logs them out.

Lastly, if the user is mid-change and has not saved their work when the automatic log out event happens, changes are lost and the application freezes to a forced close (notepad.exe in this case).

Note: as mentioned in Test Case Set 1.1, Action 5.2.A.4, for this testing, every permission rule created covered all 3 options for Login Status: Online, Offline, and PC Checkout, as shown in the example in that section.

5.2.E Since logging information can only be sent if the user is connected to the internet, explore the capabilities of the local agent to store logging information and then provide that information once a connection is restored.

5.2.E.1 Can the local agent detect when its log has been deleted or altered? Does the local agent receive acknowledgement that its log was received and accepted?

See Action 5.2.D.1 for Method.

Test environment notes:

- Windows 10 Home x 64
- Notepad.exe
- .txt File format

Successful changes that occur in the offline-but-not-yet-logged-out-of-the-desktop-client software grace period (roughly five minutes after Internet access is lost) do seem to be logged in the Fasoo system administration console after Internet access is restored. This is very unpredictable though, particularly with manually saving.

Events that occur after the client software has been automatically logged out do not appear as log entries in the administration console. For example, view attempts fail when users are offline. The desktop client software generates an unauthorized access error on view attempt through the application (notepad.exe

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.2: Local Agent—Identify Who, When, and Where

here), but no log of a 'failed' view attempt appears in the administration console online after Internet access is restored.

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.3: Browser—Identify Who, When, and Where

Overview:	The TDP can be accessed through a browser. These test cases explore the information from the DRM software when the TDP is accessed through the browser. Discover the types of information the software can furnish: ▪ Who accessed or attempted to access the TDP? ▪ Who made changes to or attempted to change the TDP? ▪ When was the TDP accessed or the attempt to access made? ▪ When were the changes or attempted changes made? ▪ Where was the TDP accessed or attempted? Where were the changes or attempted changes made?
Requirements:	R6.1, R6.2, R6.3, R25
Preconditions:	The TDP is available to be accessed, the policy set is applied to the TDP, and authorized and unauthorized user sets exist.
Postconditions:	The access log is updated showing information for the actions performed on the TDP.
Assumptions:	Tasks 1 and 3 have been completed.

Permutations

5.3.A Explore the ability for DLA to track who receives protected data.
5.3.A.1 When the supplier attempts to access the TDP, does the software log a notification with the identity of the user making the attempt?
The Fasoo FED product does not implement browser-based functionality.
5.3.A.2 What kinds of information are logged when the TDP is accessed through the browser?
The Fasoo FED product does not implement browser-based functionality.
5.3.A.3 Who is attempting to access the TDP?
The Fasoo FED product does not implement browser-based functionality.
5.3.B While the TDP is being manipulated in the browser, explore the software's ability to do the following:
5.3.B.1 Determine who is making the changes.
The Fasoo FED product does not implement browser-based functionality.
5.3.B.2 Determine who attempted to make changes but was denied by the system.
The Fasoo FED product does not implement browser-based functionality.
5.3.B.3 Determine when the changes occurred.
The Fasoo FED product does not implement browser-based functionality.
5.3.B.4 Determine where (geographic location) the changes occurred.
The Fasoo FED product does not implement browser-based functionality.
5.3.B.5 Determine how often information is logged.
The Fasoo FED product does not implement browser-based functionality.

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.4: Access a Copy of the TDP

Overview:	In these test cases, an unauthorized user has received a copy of the TDP. For example, the TDP was forwarded to the user through email. This user does not have a local agent and is attempting to access the TDP using native applications as well as through the browser. Perhaps the TDP cannot be viewed at all without local agent; can this user get a local agent? Does the software supply the same level of logging for a copy sent to an unauthorized person?
Requirements:	R15
Preconditions:	- A copy of the TDP has been forwarded, via email, to an unauthorized user. - Policy Set 2 has been applied to the TDP.
Postconditions:	The system's log files have been updated with all the possible information.
Assumptions:	Summary answers to the questions posed within the overview. - The TDP cannot be viewed, edited, etc. without the client software. - In order to get the client software, the user will need to contact DLA, create an account, then install the client software once DLA sends it.

Permutations

5.4.A As an unauthorized user, attempt to do the following.

5.4.A.1 View all the files in the TDP.

- Unable to view without the client software.
- Log entries are not created without the client software.

5.4.A.2 Change each file in the TDP.

- Unable to make changes without the client software.
- Log entries are not created without the client software.

5.4.A.3 Screenshot one or more files.

- The file cannot be opened without the client software. Therefore, no screen shots can be taken.
- Log entries are not created without the client software.

5.4.A.4 Print one or more files.

- The file cannot be opened without the client software. Therefore, the file cannot be printed.
- Log entries are not created without the client software.

5.4.A.5 Attempt to share screen over Zoom or MS Teams.

- The file cannot be opened without the client software. Therefore, the file cannot be shared.
- Log entries are not created without the client software.

5.4.A.6 Take a photo of the screen using a camera or cell phone.

- The file cannot be opened without the client software. Therefore, a picture cannot be taken.
 - If the file could be opened, there is no way to prevent a picture being taken with a cell phone.
- Log entries are not created without the client software.

5.4.A.7 Evaluate whether the same level of logging occurs when a copy of the TDP is sent to an otherwise authorized person, instead of that authorized person obtaining the TDP from DLA.

Yes, if the authorized person has the client software installed and has Internet connectivity, the same level of logging is generated.

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.4: Access a Copy of the TDP

5.4.A.8 Evaluate whether the routine maintenance process of making backup copies of files produces access log entries or entries in a log of copies made.

Log entries are not generated when a copy of a file is made. They are only generated when a user (with the client software installed and running) performs an action on the file. Background processes do not generate a log entry.

5.4.A.9 Evaluate whether logging is compatible with indexing or background processes for OneDrive, SharePoint, or other non-local file store approaches.

Log entries are only generated when a user (with the client software installed and running) performs an action on the file. Background processes do not generate a log entry.

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.5: Supply Information about Changes

Overview:	Explore the ability of the DRM software to detect the changes made to the TDP. Once the change is identified, is enough information provided to help evaluate the seriousness of the changes made to the TDP?
Requirements:	R4.1, R4.2, R4.6
Preconditions:	The original unchanged TDP has DRM Policy Set 2 applied.
Postconditions:	The TDP has been changed and the change has been reported.
Assumptions:	Task 1 has been completed.

Permutations

5.5.A Evaluate whether the DRM software can detect the changes made to the TDP.

5.5.A.1 For example, if the TDP is opened and a paragraph in one of the documents is modified—can the software point out the change?

No. The Fasoo software cannot detect the changes made to the TDP. It can only detect that a change has been made.

5.5.A.2 If the software does not have that capability, does an alternative method provide this information?

No. At this time, there are no alternative methods that can provide this information, other than MS Office software features for tracking changes made within Office files. Some CAD software may be equipped with similar track changes features, and there is utility software for comparing text files, etc.

5.5.B Discover if DLA can uncover the seriousness of the change.

5.5.B.1 Evaluating the seriousness of a change requires in-depth knowledge of the contents of the TDP. If given enough information, a subject matter expert (SME) can interpret the effect the change has on the system, part, etc.

Not applicable. Changes cannot be determined.

5.5.B.2 For example, removing the firing pin from the schematic of a rifle is likely to leave the weapon unusable and would, therefore, be a serious change but an alteration to the fabric for the rifle's sling may be minor.

Not applicable. Changes cannot be determined.

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.6: Check Identity and Validity Concurrently

Overview:	Verify that the software can perform identity checks (Task 5) and validity checks (Task 3) at the same time.
Requirements:	R9.2 (validity checks) + R2.2 (validity checks) currently + R6.1, R6.2, R10 (identity checks)
Preconditions:	1. Policy Set 1 has been applied to the TDP. 2. The TDP is posted on a website and can be readily downloaded.
Postconditions:	▪ The system can provide the identity of the user. ▪ The DLA receives an indication (a validity check) that the file delivered to the supplier user is correct.
Assumptions:	Tasks 1 and 3 have been completed.

Permutations

5.6.A With the local agent, as an authorized and unauthorized user, perform a number of tasks.

5.6.A.1 Download the TDP to your local machine.

See 5.6.A.3 for results. This task is part of the test setup.

5.6.A.2 Open the TDP using its native applications.

See 5.6.A.3 for results. This task is part of the test setup.

5.6.A.3 Describe the information given about the identity of the user.

For information on identity checks, see Test Case Set 5.2, 5.2.A.2, which explains the user information that can be provided.

- Identity checks are logged within the admin console of the policy server.
- The identity of the user viewing the file appears in the log.

5.6.A.4 Describe the validity check information given to DLA, the supplier, or both.

For information on validity checks, see Test Case Set 3.1, 3.1.A.1.

- Validity changes are manual and are of limited value.

5.6.B Through the browser, without the local agent, as an authorized and unauthorized user, do the following.

5.6.B.1 Download the TDP to your local machine.

See 5.6.B.3 for results. This task is part of the test setup.

5.6.B.2 Open the file TDP using your browser.

See 5.6.B.3 for results. This task is part of the test setup.

5.6.B.3 Describe the information given about the identity of the user.

The Fasoo FED product does not implement browser-based functionality.

5.6.B.4 Describe the validity check information given to DLA, the supplier, or both.

The Fasoo FED product does not implement browser-based functionality.

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.7: Report on User Behavior

Overview:	Baked-in usage tracking and analytics: the platform tracks user activities and behavior patterns for analytics.
Requirements:	R22
Preconditions:	The software is set and can access the TDP on which it monitors user behavior.
Postconditions:	N/A
Assumptions:	Tasks 1 and 3 have been completed.

Permutations

5.7.A How must the DRM software be set to gather behavior information? For example, must the TDP be stored in the DRM vendor's own datastore or can behavior information be gathered when the TDP is in DLA's network or the supplier's network?

Unknown. Fasoo did not provide us with this software module, despite our requesting it early on.

5.7.B Explore and explain the types of activities and behavior tracked when accessing the TDP.

See 5.7.A.

5.7.C Explore and explain the types of analytics from the software when accessing the TDP.

See 5.7.A.

5.7.D Are reports describing possible unauthorized behavior available?

See 5.7.A.

5.7.E Does the system send alerts when odd behavior is detected?

See 5.7.A.

Task 5: Collect Forensic Information and Check the Identity of the Recipient

Test Case Set 5.8: Support Investigation

Overview:	Describe the ability to support a forensic investigation with reports, logs, etc. For example, can the software report on who, what, when, and where logs were generated for a single TDP rather than the user gathering information from various locations into an ad hoc report?
Requirements:	R4.7, R0.2—auditing
Preconditions:	▪ The TDP has been accessed by authorized and unauthorized users. ▪ The TDP has been modified by authorized users.
Postconditions:	Unchanged (logs have been examined).
Assumptions:	Logs are available in the system for reports.

Permutations

5.8.A List the data that can be extracted from the system.
5.8.A.1 For an authorized user
See Test Case Set 5.2, 5.8.A.2.
5.8.A.2 For an unauthorized user
Assuming an unauthorized user does not have the client software installed, no data is produced for unauthorized access. If the client software is installed (which seems unlikely for unauthorized access), then the system collects the same data as it does for authorized users.
5.8.B List the formats in which the data can be given. Is the creation of an ad hoc report required or can a single report or reports supply the necessary information?
5.8.B.1 For an authorized user
The reports are limited to a comma-separated values (CSV) export of the log files, containing the data described in Test Case Set 5.2, 5.8.A.2.
5.8.B.2 For an unauthorized user
See 5.8.B.1. This applies but only if the unauthorized user has the client software installed.
5.8.C Explore how reports are organized. Is it by file, user, date, or location? Can reports be filtered and pivoted as a spreadsheet?
5.8.C.1 For an authorized user
A single exported CSV file with the following filters: 1. Start and end date 2. Username or ID 3. Document name 4. IP address 5. Document type (e.g., FED-N, FED-R, FED-D) 6. Document class (e.g., confidential, official use, etc.) 7. Action (e.g., view, print, edit, etc.) 8. Result (success, failure)
5.8.C.2 For an unauthorized user
See 5.8.C.1. This applies but only if the unauthorized user has the client software installed.

Task 6: DRM Software Information

Test Case Set 6.1: Integration

Overview:	This test case asks broad and high-level questions about the potential of DRM software implementation at DLA.
Requirements:	R17, R18, R19
Preconditions:	The tester has access to the DRM software and its documentation, and can reach out to the vendor, if needed.
Postconditions:	The tester answered the questions posed in this test case set.
Assumptions:	The tester reviews the DRM software documentation or discusses with the vendor to answer the questions in this test case set properly.

Permutations

6.1.A Explore the ability for the DRM software to support a large user base. A large user base involves TDPs being accessed by suppliers, not users applying DRM permissions.

6.1.A.1 Verify that scaling up the platform to meet DLAs needs would not pose a significant challenge. DLA publishes tens of thousands of items each month for procurement processing. Of the over 200,000 manufacturing firms in the United States, each may want to review a large number to TDPs per month.

Sent as ticket 1214 to Fasoo: <https://helpdesk.fasoo.com/support/tickets/1214>. The following information was provided from Fasoo:

“Fasoo has several customers with average monthly document accesses that far exceed the example LMI provided—For instance, Samsung has 700,000 users accessing protected documents within their ecosystem (170K internal users and the balance are external third parties), and the planning estimate we use based on historical averages is 50 document accesses per day, per user, which means that there are over 1 billion document accesses per month in the Samsung ecosystem.

Another example is NH Bank, they have 100,000 internal users and are averaging slightly above 20 million document accesses per month (it equates to roughly 70 document accesses per day—many users never approach this number, but some ‘power users’ and system accesses push the average up).

All to say Fasoo would feel very confident—with demonstrable performance statistics from current operationally-deployed systems by large-enterprise customers with global footprint—that the scalability of the system would be able to meet the requirements should DLA decide to protect every TDP.”

6.1.A.2 Can the system handle DRM for so many TDP accesses over several years—e.g., 20 million accesses per month = 100 lookers (potential bidders) × 7,000 procurement opportunities per day × 30 days per month?

Sent as ticket 1214 to Fasoo: <https://helpdesk.fasoo.com/support/tickets/1214>. Refer to the response from Fasoo documented in 6.1A.1.

6.1.B Explore the ability for the DRM software to integrate with DLA systems.

6.1.B.1 How easily can the DRM software pair with DLA's enterprise systems? The assumption is for DLA administrators to apply DRM policies to the TDP prior to posting it in DIBBS.

Based on the team's findings during the prototype, pairing Fasoo FED software with DLA's enterprise systems, at a high-level, appear to be straight forward. In short, implementation would involve the following:

- DLA hires Fasoo technicians or trains internal personnel in the use of the FED software
- Policy servers are created
- Policies and rules governing DRM protected files are defined
- Accounts are created
- FED client software is installed across the organization, including the devices of suppliers
- DLA personnel are trained in the use of the FED software and the rules governing its use

The team has identified several areas as potential complications. These are described below.

FED Client software requirement

The pairing of the FED with DLA's enterprise systems requires the installation of Fasoo FED client software across their internal user base. In addition, suppliers who wish to access the secured files would need the

Task 6: DRM Software Information

Test Case Set 6.1: Integration

client software installed on their devices as well. While this may appear simple from a technical standpoint, there are concerns that the suppliers would be apprehensive about installing the client software on their devices. This concern is derived from the fact that the client software takes over the device on which it is installed. During the prototype, the team discovered that the client software did not allow a document to be edited/saved without being logged into the client software. Also editing/saving files could be inhibited when connection to the Internet is broken (although editing/saving CAD files may be unaffected).

Account creation

During the prototype, the team determined that accounts can be created one of two ways: (1) manually using the admin console or (2) automatically using an LDAP. The team was unable to implement the LDAP account creation process due to various access issues between the Amazon Web Services (AWS) testing environment and Fasoo's policy server. The team worked with Fasoo engineers but were unable to resolve the issues. Based on conversations with Fasoo staff, it is the team's assumption that supplier identification (or user names) would need to reside within a public LDAP in order to connect with Fasoo's policy server to create accounts. A public LDAP raised security concerns among the team's network engineers.

A way around public LDAP would be to bring the Fasoo policy server behind DLA's firewall and require Fasoo engineers to use a DLA secure site to access the software for maintenance purposes. Once within the DLA's network, DLA network engineers could create the appropriate connections without the security issues posed by a public LDAP.

Software Support

The FED EDM software does not support all the applications DLA uses within its ecosystem, most notably Office 365, WinZip, and OpenText or Imagenation.

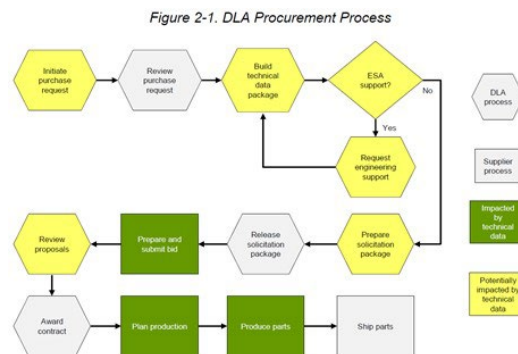
6.1.B.2 Can DRM software integrate with DLA systems (DIBBS) in other ways?

The DLA could fully integrate the Fasoo FED into their environment, encrypting all files.

6.1.C How does the implementation of DRM affect DLA processes? Would implementation significantly affect DLA processes and operations?

6.1.C.1 The relevant processes are described in the project's as-is documentation.

DRM would only affect one step in DLA's current process: "Release Solicitation Package" (see figure below)



- DLA would need to install DRM client software as required
- Implementation of DRM would significantly affect DLA processes and operations by requiring additional manual effort for encrypting solicitation packages, for ensuring that solicitations have been encrypted, for creating User IDs, for providing DRM software to potential suppliers, and for approving permissions to view or edit files, for every access of solicitation package files
- Alternatively, DLA would not need to be involved in the routine workflow of suppliers requesting access to encrypted files if the following requirements are met:
 1. DLA placed solicitations in a data store where the solicitation packages were encrypted automatically upon being placed in storage (other options, such as automatic encryption at preset times or intervals, could suffice). Requires the installation of the client software on DLA's

servers, as well as on the local machines of those who would have a need to use the secured files.⁷

2. Potential bidders can obtain the DRM client software without manual involvement of DLA personnel.
3. Potential bidders could automatically be assigned Fasoo User IDs based on their CAGE codes.⁸
4. The User IDs assigned to potential users put them in user groups where they could make provisional requests and obtain self-approval to view or edit files (or receive other pertinent permissions).⁹

* Implementation of DRM would affect DLA processes and operations by adding setup and maintenance steps, to enable automatic encryption of files placed in certain data stores, to enable assignment of Fasoo User IDs based on CAGE codes, and to create and maintain the user groups and document classes that allow suppliers to make provisional requests and obtain self-approval for pertinent permissions:

- Implementation of DRM would require new monitoring steps for checking that encrypted files contained their proper content.
- Implementation of DRM could enable other new DLA process steps, such as steps for monitoring audit logs tracking access to solicitation packages.

⁷ Note: Installing the client software could cause unforeseen issues.

⁸ Note: the team was unable to assign user IDs automatically during the prototype.

⁹ Note: the users require the FED client software to be installed on the devices accessing the secured files.

Appendix G

DRM Requirements Definition

As described in Chapter 4, we identified 51 functional requirements for securing TDPs and characterized EDRM's ability to achieve these requirements. The process for identifying requirements is described in the Requirements Definition document, which was delivered to DLA in August 2021. This document is provided in the icon below.

The icon below provides the requirements document (entitled "Digital Rights Management to Secure Technical Data Packages: Requirements Definition") that we submitted to DLA in August 2021. It describes our process for identifying the 51 requirements by which we evaluated our prototype.

DIGITAL RIGHTS MANAGEMENT TO SECURE TECHNICAL DATA PACKAGES

REQUIREMENTS DEFINITION

VERSION 1.2

VERSION DATE: 8/17/2021



Revision History

Version	Implemented By	Revision Date	Description of Change
1.0	Chuck Lorence Martin Shinko	2/15/2021	Initial document created.
1.1	Chuck Lorence Martin Shinko	6/9/2021	Peer reviewed and updated based on feedback.
1.2	Shannon Marnien Martin Shinko Chuck Lorence	8/17/2021	Final peer review and updates applied.

Contents

1. Introduction	1
2. Project Overview	2
2.1 Method	2
2.2 Assumptions and Constraints	2
2.3 System Scope	3
3 Requirements	4
Appendix A. Requirements Derived From	7
Appendix B. Scenarios and Objectives	8
B.1 Objectives	8
B.2 Scenarios	8
B.2.1 Scenario 1: Current State	9
B.2.2 Scenario 2: Protecting the TDP	9
B.2.3 Scenario 3: Protecting the TDP and Monitoring Transactions	10
Appendix C. DRM Commercial Best Practices	11
C.1 Objectives	11
C.2 Method	11
C.3 Findings: Best Practices	11
C.3.1 Establish Core EDRM and IRM Management Practices and Policies	11
C.3.2 Factor in EDRM and IRM Users	12
C.3.3 Train Users on EDRM and IRM	12
C.3.4 Layer Technology	12
C.3.5 Ensure Encryption Schemes Are Multi-Device Compatible	13

Figure

Figure 2-1. Environment Context Diagram	3
---	---

Table

Table 3-1. Requirements for Prototypes	5
--	---

1. Introduction

The Defense Logistics Agency (DLA) supplies spare parts and other materiel to the military services. To offer this service, DLA consumes technical data packages (TDPs) developed by program offices in the military services defining the materiel that DLA procures. To support competitive procurements, as necessitated by Office of the Secretary of Defense policy and federal law (the Competition in Contracting Act), DLA must furnish potential suppliers with TDPs, imparting enough information for the suppliers to submit an authoritative price quote to DLA during the solicitation process. Any entity qualified to do business with DLA should be able to access these TDPs to ensure that DLA places no additional burden on doing business with the federal government. However, once a supplier downloads a TDP, no mechanism exists for withdrawing the data or ensuring that the supplier destroys the data. If suppliers hold on to this information, bad actors could obtain large quantities of unclassified but valuable technical data if they gain access to supplier systems.

The objective of the Digital Rights Management to Secure Technical Data Packages project is to explore the ability of commercial digital rights management (DRM) products and techniques to improve the security of TDPs that DLA is required to supply to its potential suppliers in support of competitive procurements. Specifically, the project develops prototypes to validate the benefits of different techniques and create a foundation for an informed comparison between options for securing technical data.¹

As a deliverable of the Digital Rights Management to Secure Technical Data Packages project, this document defines the functional requirements for the prototypes used during the evaluation of DRM techniques (Statement of Work Section 5.0 Deliverables). The vendors who created the software used for prototyping DRM during this project supply the non-functional requirements. Therefore, this document does not record non-functional requirements.

¹ The scope of this project does not include actual implementation.

2. Project Overview

This section describes the project's method, assumptions and limitations, and scope.

2.1 Method

The requirements described in this document were developed to facilitate our evaluation of the DRM prototype using commercial off-the-shelf (COTS) software. The requirements identification process primarily relied on our experts' extensive knowledge of the state of practice for DRM. Appendix A provides some sources that document our experts' knowledge. However, to ensure that the list of requirements was as comprehensive as possible, we developed scenarios and researched to uncover additional DRM best practices with potential value to DLA's unique environment and requirements.

Our experts selected three scenarios to show the movement of TDP during the procurement process. These scenarios enabled the team to infer where DRM would be most useful for protecting the TDP. Next, our experts created scenario objectives focused exclusively on the parts of the DLA procurement process involving the exchange of technical data. While developing scenarios and objectives, the experts noted additional requirements for evaluating DRM COTS software. Appendix B contains the scenarios and objectives.

Appendix C contains a list of commercial best practices for DRM, which were consistent with what our experts had already selected.

2.2 Assumptions and Constraints

This document was written with the following assumptions and constraints:

1. The team uses these requirements to evaluate COTS software.
2. COTS software for the prototypes is accessed via a software-as-a-service (SaaS) model.
3. While building the digital thread is not part of this effort or project, it remains a consideration for future research and development.²
4. The forensic investigation into the details and purpose of changes to data protected by DRM (see requirement R4.1, which is related to tracking changes) is outside the scope of this project.³
5. Tracking data 100 percent of the time may not be possible because, in many circumstances, the authorized derivatives necessary to support subordinate processes enter the digital thread.⁴
6. Proposed solutions consider the sharing of controlled unclassified information from the government perspective and proprietary intellectual property (IP) from the business perspective.⁵

² Digital Rights Management for Technical Data Packages White Paper (WP), Objective and Scope (OAS) 1, from 1st para, December 2020.

³ WP, OAS5, from 5th para.

⁴ WP, DLA Challenges for Protecting Technical Data (CP) 2, 2nd para.

⁵ WP, Solution Space and Commercial Best Practices (SP) 4, 4th para.

2.3 System Scope

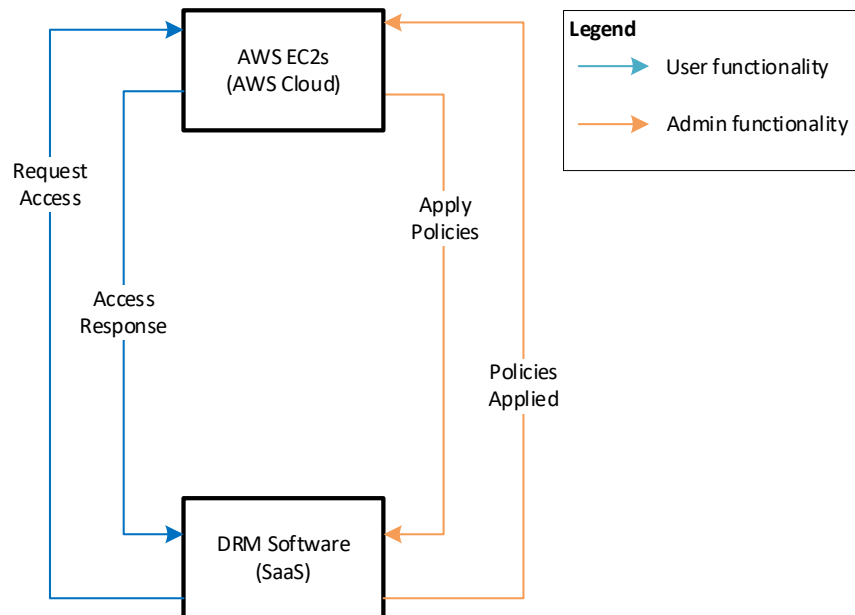
The evaluation process investigates how COTS software implements DRM practices.

The scope of the evaluation process includes those DRM-related features listed in Table 3-1. It does not include actual implementation of the prototype.

For prototyping and evaluations, participants are limited to LMI project team members. The prototypes consist of interfaces between the Amazon Web Services (AWS) Elastic Compute Cloud (EC2) testing environment, DRM software, and LMI employee laptop computers.

Figure 2-1 illustrates the high-level interoperation between the two environments.

Figure 2-1. Environment Context Diagram



3 Requirements

This project researched DRM tools, techniques, and procedures common to commercial DRM COTS products. It found techniques with the potential to benefit DLA and validated their potential use. The requirements were identified primarily using our expertise of DRM state of practice, as well as the following:

1. Scenarios created to reflect current and future DLA processes (see Appendix B).
2. Best practices from open-source research (see Appendix C).

Requirements form the basis of the project's test plan and test cases for evaluating DRM tools and techniques. The tests expand on each requirement (testing the requirements from several angles), where the team can document its findings for each. The tests themselves are exploratory, seeking to discover how DRM is implemented and highlighting any limitations and advantages when considering DRM in DLA's environment.

Table 3-1 lists the requirements for the prototype evaluations. Each requirement has a minimum of one test case for verification against the COTS software prototype. Each requirement was assigned a requirement identification (ID). The requirement ID is listed with each test case group among the test cases, indicating which group of test cases explore the requirement.

Appendix A supplies the locations from which the prototype requirements were extracted. The "Derived From" column in Table 3-1 lists the abbreviations from Appendix A. These source documents include the following:

- WP Problem Description (PD)
- WP OAS
- WP Executive Summary (ES)
- WP DLA Challenges for Protecting Technical Data (CP)
- WP SP
- WP Next Steps (NS)
- LMI DRM Technical Proposal (TP)
- LMI Report DL505T1, *DLA Can Routinely Procure Parts Using 3D PDF Files* (abbreviated as DLT5051T)
- DRM Evaluation Criteria Doc (DRM-EC).

These documents relied extensively on the knowledge of LMI's experts on the DRM state of practice.

Table 3-1. Requirements for Prototypes

ID	Requirement Description	Derived From
R0.1	The prototype leverages commercially available products, or components thereof, that require little to no tailoring to demonstrate solutions.	SP1
R0.2	Potential solutions study information encryption, management of permissions, offline access, data at rest, and auditing.	SP4
R0.3	Prototypes unlikely to result in a viable pilot project are not considered.	OAS5
R0.4	Each candidate prototype contains, in addition to prototype description, an approximated cost, time to delivery, level of effort, and likelihood of viability.	NS1
R1	DLA has the capability to advertise the procurement bid package.	PD2 (Scenario Object G)
R2.1	DLA can transfer data to many users securely, with data protected by DRM.	PD2, TP1 (Scenario Object A, C)
R2.2	DLA-transferred data has validity checks.	OAS3
R2.3	DLA-transferred data must arrive intact.	OAS1, ES1
R2.4	Data must remain intact once it arrives.	OAS1, ES1
R3.1	DRM protection offers security in transit, thwarting interception (data in transit).	OAS1, PD2
R3.2	DLA can apply access permissions to the data.	OAS3, ES1
R3.3	DLA can apply unique access permissions by user.	OAS3, ES1
R4.1	DLA can track any alterations of data protected by DRM.	PD2
R4.2	DLA can track modifications (i.e., what changed).	PD2
R4.3	DLA can determine who made the change.	PD2
R4.4	DLA can determine when the change was made.	PD2
R4.5	DLA can determine where the change was made.	PD2
R4.6	DLA can determine the seriousness of the change.	PD2
R4.7	DLA can furnish this information (R4.3–R4.6) for forensics investigation.	PD1
R5.1	DLA has control of data distribution (who can get the data).	PD1
R5.2	DLA can ensure that the data has been destroyed.	TP1
R5.3	DLA can deny access to requestors.	PD1
R6.1	DLA can track who requests protected data.	PD1, OAS1 (Scenario Object E)
R6.2	DLA can track who receives protected data (who got the data).	PD1
R6.3	DLA can track who transfers protected data.	PD1
R6.4	DLA can exercise data access revocation.	TP1
R6.5	DLA can exercise data access expiration.	PD2
R7.1	Original equipment manufacturer (OEM) users are prevented from redistributing data without permission from DLA.	PD1
R7.2	DLA is notified of attempts to redistribute data.	PD1
R8	DLA can grant permission to an OEM user to redistribute data (with data remaining under DLA control).	ES1, PD1

Table 3-1. Requirements for Prototypes

ID	Requirement Description	Derived From
R9.1	OEM users can transfer data to DLA securely, with data protected by DRM.	DL505T1 (Scenario Object B, D)
R9.2	OEM-transferred data has validity checks.	OAS3
R9.3	OEM-transferred data must arrive intact.	OAS1, ES1
R10	DLA can obtain identity checks on sources of data transferred to DLA.	OAS1
R11	OEM users can send data securely for change requests, with their data protected by DRM (data sent from the OEM to DLA, indicating to change in the TDP, e.g., engineering change request).	DL505T1 (Scenario Object F)
R12	DLA can approve change requests.	OAS1, CP3
R13	The DRM solution cannot hinder any typical external interface or the functionality expected by DLA partners and suppliers (e.g., “any typical” refers to processes, such as OEMs consuming the TDP from DLA as they do now, allowing them to verify computer-aided design drawings using software tools and create derivative products, like computer numerical control machine tool programming products).	TP4
R14	The DRM solution has a high enough level of maturity (technology readiness level) to be elevated to a pilot project with a high potential to move into production.	OAS3
R15	The DRM solution considers the practicality of preventing unauthorized disclosure through screenshots and selective copying of portions of a document.	SP4
R16.1	The platform facilitates the sharing and security of relevant file types.	EC1
R16.2	The platform facilitates the sharing and security of relevant sizes.	EC1
R17	Scaling up the platform to meet DLAs needs does not pose a significant challenge (for example, DLA publishes tens of thousands of items each month for procurement processing for the over 200,000 manufacturing firms in the United States).	EC2
R18	The platform can pair easily with DLA's enterprise systems (i.e., DLA Internet Bid Board System).	EC3
R19	The platform does not affect DLA processes and operations significantly. (The as-is documentation describes the relevant processes.)	EC4
R20	The platform integrates with DLA's data repositories, acting only as conduit.	EC8
R21	The platform presents only minor changes to DLA users' workflow.	EC9
R22	The platform tracks user activities and behavior patterns for analytics.	EC11
R23	The platform offers a feature to watermark data.	EC12
R24	The platform presents only minor change to systems and workflows of DLA partners.	EC14
R25	The platform can track the location of DLA data and user access.	EC15
R26	The platform enables DLA to automate low-level processes (to be identified) with minimal support from staff (e.g., automate setting the expiration date for a week after the bids are due).	EC16

Appendix A. Requirements Derived From

Table A-1 lists the documents from which the prototype requirements were derived. The source column names the source document and the location column pinpoints the location in the document where the requirement was found.

Table A-1. Requirements Derived From

Source	Location
LMI DRM WP, 12/31/20	Executive Summary: 1 st and 2 nd para.
	Problem Description: 1 st and 2 nd para.
	Objective and Scope: 1 st , 3 rd , 4 th , and 5 th para.
	DLA Challenges for Protecting Technical Data: 1st and 2nd para. - Top para. on page 3, 2nd para. on page 3.
	Solution Space and Commercial Best Practices: 1 st through 4 th para.
	Next Steps: 1 st para.
LMI DRM TP, May 5, 2020	Section 3.1.2 Problem Description
	Section 3.1.3, DLA Needs and Benefits, 1 st and 2 nd para.
	Section 3.1.7, Operating Environment
	Subtask 2.1 Develop Prototype Test Plan: 1st para. 1st bullet point
LMI Report DL505T1, <i>DLA Can Routinely Procure Parts Using 3D PDF Files</i>	Pg. 4-3, Section "Supplier Feedback," 4th para. under "Using 3D PDF Files to Develop a Quote"
DRM-EC	Item No. 1
	Item No. 2
	Item No. 3
	Item No. 4
	Item No. 8
	Item No. 9
	Item No. 11
	Item No. 12
	Item No. 14
	Item No. 15
	Item No. 16

Appendix B. Scenarios and Objectives

This section lists the scenarios and objectives the team used as a guide to create the requirements to evaluate the DRM prototypes. The team selected three scenarios:

1. **Current state.** A broad request for proposal (RFP) distribution of the TDP by DLA with prospective manufacturers supplying bid packages with TDPs. This scenario describes DLA's current procurement method.
2. **Protecting the TDP.** A series of transmittals between DLA and the manufacturer.
3. **Protecting the TDP and monitoring transactions.** A series of transmittals between DLA and the manufacturer using digital ledger technology to log the details of the transactions for monitoring transactions.

The following sections describe these scenarios and their objectives.

B.1 Objectives

The scenarios target one or more of the Table B-1 objectives. Together, the scenarios implement all nine objectives. The letters for each objective map the objective to the individual parts of the scenarios, as shown in the following section.

Table B-1. Objectives

Sequence Designation (for the Scenarios)	Description
A	DLA advertises the procurement under DRM, by email or posting on web page, etc.
B	Data can be transferred to many users securely.
C	Data can be transferred securely with validity checks.
D	Data can be transferred securely with identity checks and validity checks.
E	The OEM securely sends a change request under DRM. DLA approves the change by email or through a data can be transferred capability.
F	DLA maintains awareness that data remains secure and collects forensic information, as needed.
G	Data can be transferred securely in reverse.
H	Data can be transferred securely with validity checks in reverse.
I	DLA approves changes (by email or through a data can be transferred capability)—DRM is not required for in this step.

B.2 Scenarios

This section illustrates the typical DLA procurement process through simplified scenarios. Each scenario shows the movement of a TDP during the procurement process, enabling the project team to infer the most useful area for DRM integration to protect the TDP.

B.2.1 Scenario 1: Current State

In Scenario 1 (see Table B-2), DLA broadly distributes an RFP with the TDP to prospective manufacturers supplying bid packages containing TDPs. Scenario 1 is DLA's current procurement method.

Table B-2. Scenario 1

Salient Features of the Scenario	The Prototype in a Nutshell
Procurement of a manufactured part using current processes. This scenario serves as the baseline of the time and effort to procure a manufactured part and evaluate the level of confidence in the security of the technical data in transit.	• Step 1—A: DLA advertises the procurement. • Step 2—B: The TDP and proposal preparation package are made generally available. • Step 3—C: Prospective bidders validate that the TDP and proposal preparation package are valid and have not been altered.
The least expensive of the prototypes—uses current production systems and processes.	
One-way transfer. The procurement TDP (P-TDP) is available to all requesters as Distribution Statement A.	

B.2.2 Scenario 2: Protecting the TDP

Scenario 2 (see Table B-3) involves a series of transmittals between DLA and the manufacturer during the procurement process.

Table B-3. Scenario 2

Salient Features of the Scenario	The Prototype in a Nutshell
Commercial DRM technology. The DRM solution is an available commercial product rather than specially designed, custom-developed software.	• Step 1—C: DLA furnishes the P-TDP to an OEM who verifies that it has not been altered.^a • Step 2—H: The OEM submits the TDP with the bid package to DLA. • Step 3—E: The OEM submits a change request to accommodate an improved manufacturing process. • Step 4—I: DLA approves the change. • Step 5—H: The OEM submits the TDP for approval to begin manufacturing. • Step 6—H: The OEM submits technical data with objective quality evidence (OQE) for parts as manufactured. • Step 7—H: The OEM supplies the final TDP, reflecting the as-delivered condition of the product. • Step 8—H: The OEM furnishes the logistics product data model.
Controlled unclassified information. While information may be controlled, e.g., subject to export controls, its unauthorized disclosure would not reasonably be expected to damage to national security (i.e., information classified as confidential).	
Multiple transmissions of TDPs. In addition to being available to all requesters, the P-TDP may be transferred multiple times during communications with specific potential suppliers.	
TDPs undergo approved changes. Specific potential manufacturers may suggest alternatives and transmit those proposals back to DLA as altered TDPs containing their IP.	

^a Validation of the TDP for tampering is performed during each exchange and proof of safe transfer is sent to DLA.

B.2.3 Scenario 3: Protecting the TDP and Monitoring Transactions

In Scenario 3 (see Table B-4), a series of transmittals between DLA and the manufacturers during the procurement process use distributed ledger technology to log the details of the transactions to facilitate monitoring of the transactions.

Table B-4. Scenario 3

Salient Features of the Scenario	The Prototype in a Nutshell
Commercial DRM technology. The DRM solution is an available commercial product rather than specially designed, custom-developed software.	• Step 1—C: DLA supplies the P-TDP to an OEM who verifies that it has not been altered.^a • Step 2—D: DLA verifies the technical data chain of custody.^b • Step 3—H: The OEM submits the TDP with the bid package to DLA. • Step 4—E: The OEM submits a change request to accommodate an improved manufacturing process. • Step 5—I: DLA approves the change. • Step 6—H: The OEM submits the TDP for approval to begin manufacturing. • Step 7—H: The OEM submits technical data with OQE for parts as manufactured. • Step 8—H: The OEM furnishes a final TDP reflecting the as-delivered condition of the product. • Step 9—H: The OEM supplies the logistics product data model.
Commercial digital ledger technology. Traceability of which data were provided to whom and when, recorded using an available, possibly non-centralized, commercial transaction ledger product.	
Multiple transmissions of TDPs. In addition to being available to all requesters, the P-TDP may be transferred multiple times during communications with specific potential suppliers.	
Controlled unclassified information. While the information may be controlled, e.g., subject to export controls, its unauthorized disclosure would not reasonably be expected to damage to national security (i.e., information classified as confidential).	
TDPs undergo approved changes. Specific potential manufacturers may suggest alternatives and transmit those proposals back to DLA as altered TDPs containing their IP.	

^a Validation of the TDP for tampering is performed during each exchange and proof of safe transfer is sent to DLA.

^b Validation of the path of the data and validation that changes were authorized is performed during each exchange and proof of safe transfer is sent to DLA.

Appendix C. DRM Commercial Best Practices

This appendix offers an overview of the DRM best practices of commercial industry, including companies like Netflix and Verizon.

C.1 Objectives

This section reviews common enterprise digital rights management (EDRM) and information rights management (IRM) tools, techniques, and procedures in the commercial media industry. Our research on EDRM and IRM best practices focused on answering the following questions:

- What have the known DRM providers and users learned about the deployment of EDRM and IRM technology?
- How are companies deploying EDRM and IRM technology?

C.2 Method

The LMI research team searched open sources for best practices for implementing EDRM and IRM. Despite the general dearth of open-source information on EDRM and IRM best practices, we established a best practices baseline through a compilation of articles and blogs from academia, government, and the commercial sector. After extracting the most salient or recurring best practices, our research team categorized the findings.

C.3 Findings: Best Practices

The following sections detail our key findings on commercial best practice for implementing EDRM or IRM. The footnotes denote sources.

C.3.1 Establish Core EDRM and IRM Management Practices and Policies

Create oversight and governance structures. Set up an EDRM governance structure. One source suggests appointing a “data owner” or “third-party expert” to oversee DRM implementation.⁶

Establish clear roles and responsibilities. Decide the target audience of the technology, such as specific individuals, teams, or offices.⁷

Build a content selection framework. Select the content requiring EDRM and IRM; do not apply this technology indiscriminately.^{8,9}

⁶ Chiradeep BasuMallick, “What is Digital Rights Management? Definition, Benefits, and Best Practices,” Toolbox.com, December 12, 2020. Accessed September 23, 2021, <https://www.toolbox.com/it-security/identity-access-management/articles/what-is-digital-rights-management/>.

⁷ Queensland Government, “Use Digital Rights Management and Encryption,” May 5, 2021. Accessed September 23, 2021, <https://www.forgov.qld.gov.au/use-digital-rights-management-and-encryption-for-records>.

⁸ See footnote 9.

⁹ See footnote 10.

Plan for scale. Consider how protected content will be used across different platforms and devices, and design the solution accordingly. According to one source, “the less functional the display environment, the less DRM is required to control that environment.”¹⁰

Develop a DRM rollout plan. Phase EDRM implementation. Make use of pilots, proof of concept studies, and carefully selected use cases.¹¹

Define and manage security protocols. One example from our sources recommended the maintenance of “formal encryption/decryption key or password management regimes.”¹²

C.3.2 Factor in EDRM and IRM Users

Obtain user buy in. Examples include surveying prospective users, conducting a focus group, and developing an EDRM blueprint, then sending it out for user feedback.¹³

Ensure a seamless and convenient user experience. A seamless EDRM experience promotes correct and routine use of EDRM and IRM technology.¹⁴

Leverage multi-DRM solutions to support and maximize platform compatibility (video). Multi-DRM solutions have license management features for multiple DRMs, such as PlayReady, Widevine, and FairPlay, to support major web browsers and mobile operating system (OS).¹⁵

C.3.3 Train Users on EDRM and IRM

EDRM users and oversight personnel require training to install and use EDRM technology properly. This training further facilitates buy-in.¹⁶

C.3.4 Layer Technology

According to at least one source, DRM works best when used along with associated solutions like data loss prevention, digital asset management, and content management systems.¹⁷

¹⁰ Diana Holm, “Digital Rights Management Do’s and Don’ts,” FileOpen Document Security Blog, March 7, 2011. Accessed September 23, 2021, <https://www.fileopen.com/blog/bid/55094/digital-rights-management-do-s-and-don-ts>.

¹¹ Deloitte, “Towards Data-Centric Security: Enterprise Digital Rights Management,” 2021. Accessed September 23, 2021 <https://www2.deloitte.com/ch/en/pages/risk/articles/enterprise-digital-rights-management.html>.

¹² See footnote 10.

¹³ See footnote 9.

¹⁴ See footnote 9.

¹⁵ Daniel Kim, “PlayReady DRM – 5 Things to Known About DRM Technology,” Pallycon.com., 2019. Accessed September 23, 2021, <https://pallycon.com/blog/5-things-you-need-to-know-about-multi-drm-technology-part-1/>.

¹⁶ National Archives Australia, “Implementing and EDRMS – Key Considerations,” 2011. Accessed September 23, 2021, <https://www.naa.gov.au/sites/default/files/2019-09/IM-Standard-Implementing%20an%20EDRMS%20key%20considerations-V1.0%202011.pdf>, page 21–22.

¹⁷ See footnote 9.

C.3.5 Ensure Encryption Schemes Are Multi-Device Compatible

Encryption is a key facet of DRM.¹⁸ Companies like Verizon select and apply their encryption techniques to promote compatibility across devices for their streaming content.¹⁹

¹⁸ Vitrium, "Hassle-Free Content Security: How DRM can be a Simple Solution," November 24, 2020. Accessed September 23, 2021, <https://www.vitrium.com/blog/hassle-free-drm>.

¹⁹ John Bowers and Nate Cahoon, "Best Practices for Deploying DRM in a Large-Scale OTT Stack," Edgecast.com, August 20, 2020. Accessed September 23, 2021, <https://www.verizondigitalmedia.com/blog/best-practices-for-deploying-drm-in-a-large-scale-ott-stack/>.

Appendix H

Details Regarding EDRM

EDRM Policies

EDRM uses a dynamic authorization policy engine with fine-grain access, usage controls, and attribute-based policy to protect, track, and monitor data as they are being shared and consumed. These policies, which are written to apply to certain attributes (e.g., location, role, device, or type of data), provide protection and usage controls on data that varies in value and safeguarding requirements.

EDRM policies are determined based on the identity of the recipient(s); specifically, the permission and user actions granted to control recipients from specific activities like viewing, modifying, printing, forwarding, making a copy, extracting content, and expiration. Policies can be updated or revoked even after a document has been distributed.

EDRM Centralized Control and Monitoring

Another benefit of EDRM is its ability to monitor data usage. Organizations can track their files and obtain logs of every time a user attempts to access, edit, or share a file by using central policy management. EDRM technologies can remotely revoke access to files and assets in the case of, for example, the end of an external partnership or when a contract is awarded to a selected supplier. By maintaining tight controls over documents and files even after they have left a centralized repository, EDRM allows for greater protection, even when working with partner organizations, and reduces risk of data leakage. Internally, EDRM's centralized repository nature and access logging features ensure that organization members' files and assets are the most up-to-date collaborative versions.

EDRM and the Local Client

The perfect EDRM solution would provide all the cybersecurity benefits of EDRM without requiring DLA's suppliers to install software on their devices. Unfortunately, for EDRM to provide its full benefits (beyond the ability to securely view documents), suppliers must install a local client software module on their device.

EDRM software is unique in its ability to enforce highly granular permission sets on data files while they are being used. To accomplish this, the EDRM software must be able to exert control of the inner workings of the software that is using the protected file, such as by running as a service in the background of a Windows OS with full permissions. The local client module merges with the software using the file, such as MS Word, and disables the functions the user is not authorized to enact upon the file, according to that user's permissions. The client itself communicates directly with the EDRM Policy Server to determine the user's permissions, based on the user's login information.

For example, if a user does not have editing permissions on an MS Word file, then the EDRM local client would disable all functionality that would allow a user to edit an MS

Word file. It is important to note that the control over MS Word would only take effect when an EDRM-protected file is being manipulated.

EDRM Browser-based Solutions

Control of a local third-party application can only occur with a locally installed EDRM client module. This fine-grained control functionality cannot be implemented using a browser-based EDRM implementation. Browser-based implementations can only control the actions a user can perform within a browser, and even then, they cannot control printing, screen capture, file saving, and online meeting sharing features of the browser software.

Some EDRM approaches use browser add-ons or even provide an EDRM version of browser software, thus avoiding an intrusive local client module. However, these approaches still involve what amounts to installing a local client (by way of browser software).

Another approach to providing EDRM is to use web-based applications that seem functionally identical to the data's native software. These applications may render data in a similar manner as the native application software, but the unknown differences can compromise user productivity. Furthermore, not all native application software offers a web-based equivalent functionality, and third-party offerings are not guaranteed to match the required capabilities of the original software they imitate.

EDRM Benefits and Limitations

EDRM helps to protect restricted content when it is at rest, in transit, and—unique to EDRM—in use. This presents clear benefits, such as:

- Encryption applied is nearly impossible to break.
- Files can be protected, then delivered via any normal means.
- Users can use files (view, edit, print, etc.) while they are under protection.
- Organizations can identify who can and cannot access the files within their organization, and the actions individuals can perform.
- Organizations can share files with partner organizations, but only individuals with access can perform actions on the files. In addition, organizations can limit the user access to specific actions like viewing, editing, printing with watermark, copying, and more, and can set up role-based access.
- Organizations can deny users access to a file and set access expiration dates.
- Organizations can set up EDRM to automatically protect documents when they are created, without any actions required of the creator.

These characteristics make EDRM useful in helping organizations securely share and process large amounts of information using different file types.

Although there are many benefits to EDRM, there are also several limitations. These include:

- Browser-based EDRM is typically limited to “view only.”

- Manipulating (e.g., editing) a document while it is still protected by EDRM requires a local client.
- Actions are only logged if a local client is installed and active.
- EDRM software cannot work with all file types. It may be able to protect software delivery, but the protection would need to be removed prior to accessing the file.
- EDRM COTS software does not include the functionality to provide validity checks.¹
- EDRM cannot identify exactly what was changed in a document. This would require the EDRM software to have very precise and intimate interactions with many different software types, including most CAD tools, MS Office, Adobe PDF, and more.
- EDRM cannot ensure that TDPs are destroyed.

¹ A validity check involves comparing what has been received against what has been sent for authenticity.

Appendix I

Abbreviations

3D	Three dimensional
ADI	Automated Data Integrity
AI	artificial intelligence
API	Application Programming Interface
AWS	Amazon Web Services
CAD	computer-aided design
CMMC	Cybersecurity Maturity Model Certification
COTS	commercial-off-the-shelf
CUI	Controlled Unclassified Information
DAM	Digital Asset Management
DIBBS	DLA Internet Bid Board System
DLA	Defense Logistics Agency
DoD	Department of Defense
DRM	digital rights management
EC2	Elastic Compute Cloud
EDRM	enterprise DRM
ESA	Engineering Support Activity
IaaS	Infrastructure as a Service
IP	Internet Protocol
ML	machine learning
N/A	not applicable
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
OOTB	out of the box
OS	Operating System
PR	purchase request
P-TDP	procurement TDP
QLDB	Quantum Ledger Database
R&D	research and development
RFP	request for proposal

SME	subject matter expert
TDP	technical data package
ZT PfMO	Zero Trust Portfolio Management Office

CONTACT

Robert Love

Vice President, Department of the Navy

+1.703.245.6055 *office*

robert.love@lmi.org

LMI | 7940 Jones Branch Drive, Tysons, VA 22102

About Us

LMI is a consultancy dedicated to powering a future-ready, high-performing government, drawing from expertise in digital and analytic solutions, logistics, and management advisory services. We deliver integrated capabilities that incorporate emerging technologies and are tailored to customers' unique mission needs, backed by objective research and data analysis. Founded in 1961 to help the Department of Defense resolve complex logistics management challenges, LMI continues to enable growth and transformation, enhance operational readiness and resiliency, and ensure mission success for federal civilian and defense agencies.

➔ **Learn more at lmi.org**