SYM-AM-25-305

Excerpt from the Proceedings of the Twenty-Second Annual Acquisition Research Symposium and Innovation Summit

Wednesday, May 7, 2025 Sessions
Volume I

Integrated Digital Maturity Pathway for Technical Data Packages

Published: May 5, 2025

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

Integrated Digital Maturity Pathway for Technical Data Packages

Darryl Draper-Amason, PhD—is a leading expert in Performance Improvement, leveraging her PhD in instructional systems to enhance organizational effectiveness. Her research in maturity models, instructional design, and online education has transformed training effectiveness and readiness metrics. She specializes in Performance Improvement frameworks, guiding organizations through transitions and process optimizations. [ddraper@odu.edu]

Michael McGrath, DSc—is an independent consultant with broad government and industry experience in acquisition and technology management. He has served in VP positions and corporate boards at several technology companies. His government experience includes senior positions in OSD, DARPA, and in Navy as the DASN(RDT&E). He is a consultant for the University of Maryland Applied Research Lab for Intelligence and Security. His technology interests are in manufacturing, digital technical data and data analytics. Dr. McGrath holds a doctorate in operations research from George Washington University. [mmcgrat1@stevens.edu]

Abstract

A major challenge in technology transition is the Department of Defense's (DoD) requirement for a complete Technical Data Package (TDP) with intellectual property (IP) licenses for life-cycle use. Contractors often withhold proprietary details, including manufacturing trade secrets and sensitive IP, making TDPs incomplete or outdated. Negotiating royalties for items developed with mixed government and industry funding further complicates acquisition. As a result, industry seeks to protect its IP, while the DoD faces sustainment challenges due to limited access to critical data.

This research presents a case study from the National Defense Industrial Association's (NDIA) Digital Manufacturing Working Group (DMWG), exploring how digital transformation can address these challenges. The study applies the Integrated Digital Maturity Pathway (IDMP) framework, assessing how enterprises—suppliers, prime contractors, and government agencies—can achieve greater digital interoperability despite varying levels of digital maturity. The research evaluates use cases, process improvement roadmaps, and industry–government collaboration outcomes.

Findings highlight the potential for IDMP to enhance digital TDP practices, ensuring more effective data-sharing mechanisms. This study provides insights into the broader applicability of IDMP for digital transformation, with expected benefits in acquisition efficiency, data governance, and sustainment readiness across the DoD enterprise.

Introduction

The transition of technology in defense acquisition is contingent upon the availability of complete, interoperable, and life-cycle-ready Technical Data Packages (TDPs). These packages must reconcile contractor IP protection with DoD life-cycle needs. However, disparities in digital maturity among stakeholders, suppliers, prime contractors, and government entities complicate the effective development and use of TDPs.

This paper introduces the Integrated Digital Maturity Pathway (IDMP) framework as a novel approach to overcoming these challenges. By incorporating storytelling through user stories and leveraging the Air Force's VAULTIS framework, the research integrates diverse perspectives to address systemic issues in the development of TDPs and broader digital transformation efforts.

Research Problem and Question

Research Problem

The research issue is the challenge in transitioning technology due to the requirement for a complete Technical Data Package (TDP) and an IP license that allows life-cycle use. Contractors are often hesitant to provide proprietary or sensitive details, such as trade secrets, in the TDP, especially when items are developed with mixed funding sources (government and industry). These complexities, including royalty fee negotiations, create a protectionist stance from the industry, often resulting in the DoD receiving incomplete or outdated TDPs that fail to meet its needs.

Research Question

How can digital transformation, through an Integrated Digital Maturity Pathway (IDMP) framework, facilitate the creation of robust, interoperable TDPs that protect contractor IP while fulfilling DoD requirements?

Primary Research Sources: This study utilizes the National Defense Industrial Association's (NDIA) Digital Manufacturing Working Group (DMWG) data and analysis, focusing on digital transformation strategies for technical data interoperability. Primary sources include case studies of varied enterprises (suppliers, primes, government) at different stages of digital maturity. The research also incorporates industry and government feedback on implementing the IDMP framework to assess process improvements.

Background and Problem Statement

Technical Data Packages (TDPs) serve as the foundation of sustainment, spares manufacturing, and modernization efforts in defense acquisition. A TDP contains the essential technical information required to produce, maintain, and modify a system or component throughout its life cycle. These packages typically include engineering drawings, specifications, design models, and related technical documentation, ensuring that the DoD and its contractors have the necessary data to sustain critical systems independently of the original manufacturer. The TDP content is specified by MIL-STD-31000 (DoD, 2018) to include models, drawings, associated lists, engineering design data, specifications, standards, performance requirements, quality assurance provisions, software documentation, and packaging detail. Although the MIL-STD-31000 focus is on product definition data rather than manufacturing, the DoD often requires delivery of details of unique processes (i.e., not published or generally available to industry) when essential to design and manufacture. As used in this paper, the term TDP includes such details.

The availability of comprehensive, accurate, and up-to-date TDPs is essential for ensuring operational readiness, cost-effective maintenance, and long-term sustainment of defense assets. When properly structured and accessible, TDPs reduce dependency on original equipment manufacturers (OEMs), facilitate competitive procurement processes, and enable rapid response to mission-critical repair and sustainment needs. Furthermore, as the defense industry shifts toward digital engineering and model-based systems engineering (MBSE), the role of digitally mature TDPs becomes even more critical in integrating emerging technologies like additive manufacturing, artificial intelligence (AI), and predictive maintenance into sustainment strategies.

However, the efficacy of TDPs is frequently undermined by intellectual property (IP) challenges, incomplete documentation, and lack of interoperability across the DoD and its industrial partners. These issues present significant barriers to achieving the digital transformation necessary to modernize defense acquisition and sustainment operations.

Challenges of IP Protection and Contractor Reluctance to Share Proprietary Data

One of the most persistent challenges in TDP management is the tension between government data needs and contractor IP rights. Many defense systems are developed under mixed-funding models, where both private industry and the government contribute to research and development (R&D) efforts. When contractors invest private capital into product development, they seek to protect proprietary technical data, trade secrets, and competitive advantages by limiting the level of detail included in TDPs that might be disclosed to competitors.

This reluctance to share proprietary data often leads to incomplete or outdated TDPs, hindering the DoD's ability to maintain and sustain critical systems independently. Without access to comprehensive TDPs, the government is forced to rely on sole-source contracts, leading to higher costs, reduced competition, and increased lifecycle risks. Additionally, negotiating data rights and royalty fees for intellectual property developed under government contracts remains a contentious process, further complicating the development of interoperable, accessible, and lifecycle-ready TDPs.

The implications of inadequate TDPs extend beyond sustainment costs—they also impact the DoD's ability to leverage emerging manufacturing technologies such as additive manufacturing. Without sufficient technical data, DoD depots and sustainment centers cannot fabricate replacement parts, perform structural modifications, or integrate new capabilities, ultimately affecting mission readiness and supply chain resilience.

In this context, balancing contractor IP protection with the DoD's need for technical data remains a key challenge. Current acquisition policies and contract data requirements must evolve to ensure that contractors are incentivized to share critical data, while also safeguarding proprietary innovations that drive industry investment in new defense technologies.

The Need for the Integrated Digital Maturity Pathway (IDMP) to Address These Challenges

To navigate the complexities of TDP accessibility, IP protection, and interoperability, the Integrated Digital Maturity Pathway (IDMP) framework provides a structured digital maturity approach that systematically enhances the Department of Defense's (DoD) ability to manage, share, and utilize technical data. IDMP serves as a strategic roadmap for digital transformation within the TDP ecosystem, ensuring that data is Visible, Accessible, Trustworthy, and Interoperable across the defense industrial base while balancing the needs of contractors and government stakeholders.

The IDMP framework (see Figure 1) is designed to establish a progressive, scalable approach to digital maturity, allowing the DoD and industry partners to assess their current data capabilities and implement targeted improvements in TDP management. By integrating IDMP, the DoD can facilitate secure, interoperable, and life-cycle-ready TDPs that support sustainment, manufacturing, and next-generation digital engineering.

IDMP Level	Current State	Issues	Capabilities	Objectives
Initial Level: Current Process (Manual and Basic Processes)	The government specifies delivery of a Tech Data Package (TDP) for manufacturing components, but the TDP is often incomplete, causing issues for competitive procurement.	-Incomplete TDPs: Current processes result in insufficient technical data for competitive procurement. -Vendor lock: The government is often reliant on a single supplier due to incomplete TDPs. -Data Gaps: Vendors struggle with insufficient engineering details for manufacturing, leading to fewer competitive bids and higher risks of no-bid decisions.	-Establish basic TDP standards using MIL-STD-31000 to define minimum deliverables. -Initial efforts to incorporate basic TDP requirements into contracts to improve future procurement competitiveness.	Establish clarified TDP requirements and update contract deliverables to ensure complete, competitive TDPs for future procurement needs.
Initial Level: Decisions	-Determine minimum TDP requirements to avoid gaps that cause vendor lock. -Decide if manual processes for TDP validation are sufficient or if early digital initiatives should be introduced.			

Figure 1: Integrated Digital Maturity Pathway (IDMP) Level 1 User Story # 48 (Draper-Amason, 2024).

Key Benefits of IDMP in TDP Management

IDMP addresses data interoperability by enabling the development of standardized data formats, metadata protocols, and secure digital environments, ensuring that TDPs can be seamlessly integrated across government and contractor systems. It establishes a common digital maturity framework that highlights issues affecting interoperability between legacy and emerging digital systems.

When applied to TDPs, the IDMP framework highlights mitigating IP risks through secure data-sharing mechanisms by incorporating secure data-sharing models, including Digital Rights Management (DRM), role-based access control (RBAC), and blockchain-based verification. These mechanisms help contractors retain control over proprietary data while allowing the DoD to access necessary sustainment and life-cycle management information without compromising sensitive IP.

At higher levels of maturity, IDMP addresses additive manufacturing and AI-Driven Sustainment to ensure that TDPs are machine-readable and optimized for integration with additive manufacturing (AM), predictive maintenance, and AI-driven sustainment models. This enhances the DoD's ability to rapidly fabricate parts, conduct in-field repairs, and improve logistics planning through digital twin technologies.

The TDP IDMP provides a structured governance framework for TDPs, incorporating role-based access, digital audit trails, and compliance automation. This ensures that technical data remains authoritative, up-to-date, and protected across its entire life cycle. The framework also enables automated compliance verification to align with evolving DoD data policies and acquisition regulations.

Literature Review

The Role of Technical Data Packages (TDPs) in Defense Acquisition

Technical Data Packages (TDPs) are fundamental to the sustainment, manufacturing, and life-cycle management of defense systems. A TDP provides the necessary engineering documentation, including design specifications, drawings, manufacturing instructions, and quality assurance criteria, to support the production, modification, and maintenance of military assets. Without a complete and accessible TDP, the Department of Defense (DoD) and its

sustainment partners face significant challenges in independently managing the life cycle of critical defense systems (McKay et al., 2021).

In defense acquisition, TDPs ensure that multiple vendors can competitively bid for contracts, thereby reducing sole-source dependencies and fostering a more resilient supply chain. For example, in the Amphibious Combat Vehicle (ACV) program, the U.S. Marine Corps has faced difficulties in identifying alternative manufacturers because the original contractor, BAE Systems, retains exclusive rights to the vehicle's technical data. As a result, prospective manufacturers must design and build vehicle variants without access to the TDP, increasing costs and technical risks (Wilson, 2023). This situation illustrates the critical role that TDPs play in ensuring that sustainment and future acquisitions remain cost-effective and adaptable to evolving operational requirements.

Existing Limitations in TDP Accessibility, Completeness, and Interoperability

Despite their importance, TDPs often suffer from accessibility and completeness issues, largely due to restrictions in intellectual property (IP) rights and the proprietary nature of many defense systems. A major limitation is that program managers (PMs) frequently do not procure sufficient data deliverables and associated data rights upfront, which can severely restrict the DoD's ability to sustain weapon systems over the long term (Harper, 2017). The Defense Acquisition University (DAU) emphasizes that acquiring the correct level of TDP access is essential for long-term sustainment but acknowledges that many program managers lack clear guidance on how to structure their procurement strategies for technical data rights. This has led to cases where the DoD is locked into long-term contracts with original equipment manufacturers (OEMs) who retain exclusive control over sustainment operations.

Another major issue is interoperability, particularly in large-scale programs that involve multiple stakeholders and contractors. Engineering design descriptions within TDPs are often developed in proprietary formats, making it difficult to integrate and modify data across different systems and sustainment environments (McKay et al., 2021). The complexity of maintaining configuration consistency across different versions of TDPs further complicates sustainment operations. Research highlights the need for improved digital product life-cycle management tools that can help engineers maintain TDP consistency while adapting designs to evolving mission requirements.

Additionally, many legacy defense systems were originally designed without consideration for future digital sustainment capabilities, making it difficult to apply modern manufacturing techniques such as additive manufacturing (AM) and AI-driven predictive maintenance. When TDPs are incomplete or not machine-readable, the ability to leverage advanced digital manufacturing techniques is significantly reduced. In some cases, defense sustainment depots have resorted to reverse engineering components due to the lack of available technical data, an expensive and time-consuming process that could have been avoided with proper TDP procurement strategies (Harper, 2017). The lack of accessibility, completeness, and interoperability in TDPs presents significant challenges to defense sustainment and manufacturing. As demonstrated in the USMC's ACV program, failure to secure full technical data rights from the outset can limit competitive procurement options and increase sustainment costs. Likewise, deficiencies in TDP structure and standardization hinder the adoption of modern digital sustainment technologies, making it harder for the DoD to fully leverage AI, additive manufacturing, and predictive analytics.

Digital Maturity and Data Interoperability Challenges

The increasing complexity of defense acquisition and sustainment demands a structured approach to digital maturity that enables organizations to assess their current capabilities, identify gaps, and implement targeted improvements. As the DoD advances toward digital

transformation, the ability to integrate technical data, cybersecurity measures, and data-sharing protocols across different stakeholders remains a critical challenge. Without a standardized framework to guide this transformation, organizations risk data fragmentation, inconsistent governance, and cybersecurity vulnerabilities, ultimately undermining operational readiness and sustainment efficiency.

A structured digital maturity framework is essential for ensuring that data governance, security, and interoperability are addressed holistically. Kırmızı and Kocaoglu (2022) highlight that organizations benefit from a digital transformation maturity model that establishes measurable stages of digital adoption, allowing them to implement structured improvements rather than ad-hoc, reactionary changes. This model provides a roadmap for organizations to evolve from manual, siloed processes to fully integrated digital ecosystems that facilitate secure, efficient, and scalable data sharing. Within the DoD, the Integrated Digital Maturity Pathway (IDMP) serves as such a framework, guiding stakeholders through progressive stages of digital maturity that enhance TDP management, interoperability, and cybersecurity measures (Kırmızı & Kocaoglu, 2022).

Despite the potential benefits of digital maturity models, significant barriers to data interoperability persist across defense and industrial partnerships. Many legacy defense systems were not designed with modern digital architectures in mind, creating compatibility issues between older, proprietary formats and emerging model-based systems engineering (MBSE) standards. This lack of interoperability leads to data silos, where critical technical information remains locked within specific platforms, inaccessible to external stakeholders who require it for sustainment and modernization efforts. Research on data leakage prevention (DLP) and cybersecurity maturity further indicates that defense organizations struggle with balancing data accessibility with security, as proprietary data-sharing restrictions often hinder effective collaboration between DoD entities and private contractors (Domnik & Holland, 2024).

Compounding these challenges is the growing risk of cyber threats targeting defense networks and digital assets. Al Shidhani (2019) underscores the importance of cybersecurity maturity models, noting that organizations must progress through structured digital transformation phases to achieve secure and interoperable data environments. The DoD's digital maturity trajectory reflects these challenges, necessitating a comprehensive approach to data protection that ensures secure yet accessible technical data exchanges while mitigating the risks of data breaches, insider threats, and unauthorized access (Al Shidhani, 2019).

To address these issues, the IDMP framework provides a structured, security-focused roadmap for the DoD's digital transformation efforts. By incorporating cybersecurity best practices, governance policies, and data interoperability standards, IDMP enables the DoD to establish secure, standardized data-sharing mechanisms that protect technical data integrity while maintaining accessibility for authorized users. This framework not only enhances TDP management and supply chain resilience but also ensures that digital transformation efforts align with evolving cybersecurity and data governance regulations.

Through a structured approach to digital maturity and data interoperability, the DoD can transition toward a more resilient, secure, and data-driven sustainment strategy, leveraging IDMP to overcome the challenges of legacy system constraints, data silos, and cybersecurity vulnerabilities. As prior research suggests, the adoption of maturity models such as IDMP can serve as a critical enabler of digital transformation, ensuring that defense organizations remain adaptive, secure, and operationally effective in an increasingly digital landscape.

Addressing These Challenges with the IDMP Framework

The IDMP framework provides a structured approach to overcoming digital maturity and interoperability challenges within the DoD and its industry partners. By implementing

progressive maturity levels, the framework systematically guides organizations through various phases of digital adoption, ensuring a measured and strategic transformation toward a fully integrated and interoperable data environment.

In addition to establishing a digital maturity roadmap, IDMP aligns with key data security standards by integrating cybersecurity principles and VAULTIS protocols, reinforcing data governance policies and risk mitigation strategies. This structured approach ensures that digital assets remain both accessible and secure against evolving cyber threats, allowing for controlled and compliant data management across different stakeholders.

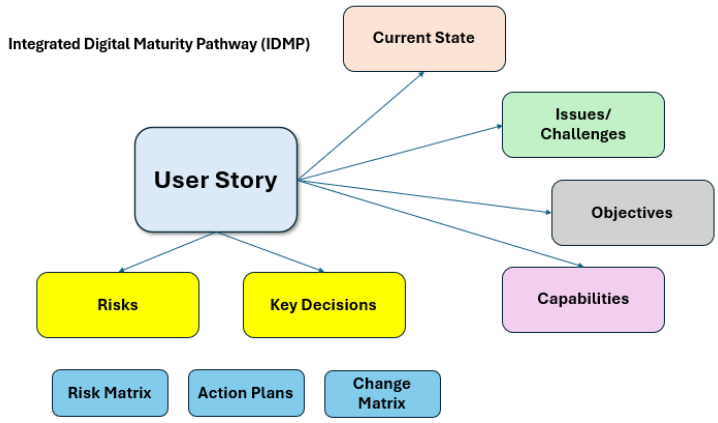

Figure 2: Integrated Digital Maturity Pathway (IDMP) Components (Draper-Amason, 2024).

To further enhance digital transformation efforts, the IDMP framework incorporates additional tools that aid in implementation, sustainability, and scalability. These tools include the Organizational Change Matrix, Risk Matrix, and Action Planning framework, each of which plays a critical role in guiding organizations through the challenges of digital transformation (Figure 2).

The Organizational Change Matrix assists organizations in assessing cultural and operational readiness for digital adoption, identifying potential barriers, change drivers, and necessary interventions to facilitate smooth transitions. By systematically analyzing stakeholder engagement, leadership support, and workforce adaptability, this tool enables organizations to strategically implement digital maturity models while fostering an environment conducive to long-term adoption and growth.

The Risk Matrix provides a structured method for identifying, assessing, and mitigating risks associated with digital transformation efforts. Given the complexities of technical data management, interoperability, and cybersecurity, this tool enables organizations to proactively address potential vulnerabilities, compliance risks, and integration challenges. Through risk prioritization and mitigation strategies, organizations can make informed decisions that minimize operational disruptions and sustainment risks during IDMP implementation.

Additionally, the Action Planning framework serves as a roadmap for execution, ensuring that digital transformation initiatives remain goal-oriented, measurable, and scalable. This structured approach supports milestone tracking, resource allocation, and performance evaluation, enabling organizations to sustain momentum and continuously improve digital capabilities over time. Action planning also helps to align IDMP implementation with broader DoD modernization objectives, ensuring that stakeholder coordination and policy compliance remain integral to digital maturity progress.

To further enhance secure data exchange, IDMP implements standardized, interoperable mechanisms that eliminate data fragmentation and security vulnerabilities. Through structured data-sharing protocols, the DoD and its partners can streamline access to critical technical data, improve collaboration between defense agencies and contractors, and strengthen supply chain resilience.

By leveraging IDMP as a structured digital maturity framework, the DoD can enhance TDP accessibility, improve supply chain efficiency, and enable secure, data-driven decision-making across defense acquisition and sustainment ecosystems. The incorporation of organizational change strategies, risk mitigation methodologies, and structured action planning ensures that digital transformation efforts are not only implemented effectively but also sustained and scalable. This comprehensive approach ensures that technical data remains both operationally effective and protected, supporting mission-critical sustainment activities while advancing the DoD's digital modernization goals.

User Stories

User stories capture end-user perspectives and operational challenges, providing a structured mechanism to define and prioritize capabilities within the IDMP framework. This approach allows for iterative refinement, ensuring that the IDMP remains adaptable to evolving technological and organizational needs.

As Cohn (2004) describes, user stories are simple, concise representations of system functionality expressed from the user's perspective, which help to drive agile development and ensure stakeholder alignment. They serve as a means of communication between developers, end-users, and decision-makers, helping to capture key functionalities in a format that is both understandable and actionable. The IDMP benefits from this approach by structuring digital maturity progression based on clearly articulated user needs, facilitating the alignment of technical capabilities with operational objectives.

User stories have been widely used in agile methodologies, such as Scrum and eXtreme Programming (XP), to facilitate a user-centered approach to software and systems development. Wautelet et al. (2017) emphasize that user stories serve as operational requirements representation models that drive transformation within a particular development paradigm. Their research highlights how user story's structure system development, allowing for an incremental and adaptable approach to digital transformation within frameworks like IDMP.

Beyond software engineering, user stories have also been used as a mechanism for measuring value in complex systems. For instance, research on nursing value user stories has demonstrated how this methodology can be applied to link specific actions to measurable outcomes, highlighting its broader applicability beyond software development. Similarly, within the IDMP framework, user stories can help quantify the impact of digital transformation initiatives by providing traceability from requirement definition to implementation outcomes.

The structured nature of user stories ensures that digital transformation initiatives, such as those encompassed by IDMP, are aligned with best practices in requirements engineering. Lucassen et al. (2016) outlines the INVEST framework (Independent, Negotiable, Valuable, Estimable, Small, and Testable), which defines key principles for writing high-quality user stories that improve clarity, prioritization, and testability. The integration of well-defined user stories into IDMP, organizations can enhance their ability to manage change, mitigate risks, and drive measurable improvements in digital capabilities (see Figure 2).

Ultimately, the integration of user stories within the IDMP framework provides a structured and scalable approach to digital transformation, ensuring that technological advancements are driven by stakeholder needs, operational requirements, and best practices in

digital maturity modeling. The use of user stories as foundational elements of IDMP not only enhances requirements clarity and system adaptability but also ensures that digital maturity advancements remain user-driven, measurable, and aligned with operational goals.

These stories served as the foundation for the working group's application of the IDMP framework. The richness of these cases lies in their ability to highlight both commonalities and nuances, enabling the validation of the IDMP framework and the identification of targeted solutions.

The Role of the VAULTIS Framework

The Air Force's VAULTIS (Visible, Accessible, Understandable, Linked, Trustworthy, Interoperability and Secure) framework (Table 1) served as a guiding model for structuring and refining user stories. VAULTIS emphasizes the integration of advanced technologies, secure data-sharing protocols, and interoperability across diverse systems. Drawing from VAULTIS principles, this study adopted a structured approach to capturing user stories.

Table 1. VAULTIS Framework USAF

Visible	Ensuring that all critical data, processes, and dependencies are transparently available to stakeholders to support informed decision-making throughout the lifecycle of technical data management.
Accessible	Guaranteeing that authorized stakeholders can seamlessly retrieve necessary information when and where it is required, minimizing delays and barriers to effective use.
Understandable	Presenting data and processes in a format that is clear, consistent, and interpretable by both technical and non-technical stakeholders, ensuring alignment across diverse teams.
Linked	Establishing robust connections between datasets, systems, and processes to enable integration, reduce redundancies, and create a comprehensive digital thread for lifecycle management.
Trustworthy:	Building confidence in the integrity, accuracy, and authenticity of the data and systems to foster reliance on the framework for critical decision-making.
Interoperable:	Facilitating seamless communication and functionality across different systems, platforms, and stakeholders, regardless of varying digital maturity levels.
Secure:	Implementing rigorous safeguards to protect data and intellectual property from unauthorized access or misuse, ensuring compliance with contractual and regulatory requirements.

This alignment provided a robust foundation for developing user stories that address the specific challenges of TDP development and digital transformation.

Case Study Methodology in Digital Transformation Research

Qualitative research methods are used to uncover the direct actions and experiences of individuals in a social activity they carry out (Bryman, 2008; Mutch, 2005). Johnson and Christensen (2008) posit that these methods are valuable because they "view human behavior as dynamic and changing, and advocate studying phenomenon in depth and over an extended period of time" (p. 388). Qualitative approaches used in this study included working group discussions, a workshop, document review, user story contributions that include experiences of

the working group participants and their direct actions associated with their experiences to enhanced understanding of a particular user story of the study inquiry.

Case studies are a powerful research methodology that allows for in-depth exploration of complex phenomena within real-world contexts. Yin (2014) posits that case studies are particularly valuable in addressing "how" and "why" questions, making them ideal for exploring the multifaceted challenges of digital transformation and TDP practices. According to Yin (2003), a case study design should be contemplated when four criteria are met. First, the answer to the "how" and "why" questions. Second, the individuals who are involved in the study cannot be manipulated. Third, to reveal contextual conditions with the belief that they are relevant to the phenomenon under investigation. Fourth, there are unclear boundaries between the phenomenon and context. For example, in this study, the case is the identification of user stories from the context of the government manufacturing community. It is within this setting that the user stories were developed and utilized. It would be impossible to have a correct picture of the development of user stories without considering the context.

NDIA and the Digital Manufacturing Working Group

The National Defense Industrial Association (NDIA) is a prominent 501(c)(3) educational nonprofit organization dedicated to promoting national security by facilitating collaboration among industry, government, and academia. The NDIA Manufacturing Division formed a Digital Manufacturing Working Group (DMWG) in 2024 to address digital transformation effects on manufacturing throughout the life cycle, with an emphasis on technology-enabled changes at the interface between industry and government.

DMWG User Stories Related to TDPs

To determine member interests, the DMWG captured user stories expressed as "As a (insert role), I want to (insert use of digital data), to achieve (insert benefit)." The initial set of 80 user stories ranged from interests in IP rights and TDP uses, to configuration management, to digital twins for manufacturing and supply chains, and to data analytics for Industry 4.0. An initial subset of five user stories was selected as the focus for a November 2024 workshop on manufacturing uses of technical data, as shown in Table 2.

Table 2. User Stories Related to TDP Delivery to the DoD

User story 16 & 20	As (16) a Supplier or (20) the Prime Integrator of a Supply Chain	I want to protect my proprietary data and that of my suppliers from disclosure or use outside specifically negotiated license provisions,	So that I can share data and models for collaboration within the supply chain and with the Government and ultimately provide better products and services.
User story 47	As a Prime Contractor	I want to offer Tech Data as a Service (TDaaS) as an alternative to data deliverables	So that my government customer will have secure access to up-to-date tech data for sustainment at the time of need.

User story 48	As a Government Product Support Manager	I want to get delivery of a complete tech data package with unlimited data rights	So that I can release build-to-print information for competitive procurement of spare parts
User story 49	As a Government Depot Manager	I want to have access to digital design and manufacturing data	So that I can accomplish depot repairs and fabricate parts as needed (additive and other mfg processes)

These user stories served as the foundation for the working group's application of the IDMP framework. The richness of these cases lies in their ability to highlight both commonalities and nuances, enabling the validation of the IDMP framework and the identification of targeted solutions. Workshop participants clarified user story boundaries, identified problems and mitigation strategies, and identified barriers to the widespread implementation of digital transformation ideas.

2024 Workshop Results

A central theme of the workshop was that DoD attempts to negotiate TDP deliverables and associated data rights years before specific sustainment needs are known. Consequently, the DoD tends to require that all relevant technical data be bought, ideally with unlimited rights, to be prepared for any need that may arise downstream. Industry lacks insight as to what the DoD will ultimately do with the TDP, makes the worst case assumption of disclosure to competitors, and fights hard to protect proprietary data. Digital engineering greatly expands the range of data that might be included in a TDP. At the same time, digital transformation offers new opportunities.

Ideas generated during the workshop centered on ways digital transformation can enable new ways of developing, protecting, delivering and using technical data. Examples include:

- User Stories 16 & 20: Start to implement role-based secure access and Digital Rights Management (like DRM in the music and movie industries) in Product Lifecycle Management (PLM) and other automated TDP systems. Evaluate prototype blockchain solutions to give prime contractors and suppliers more visibility and control over IP protection. Use generative artificial intelligence (Gen AI) to assist in proprietary markings in documents containing IP.
- User Story 48: Better define the TDP using MIL-STD-31000 Option Selection Worksheet and a 2-page Data Item Description (DID) rather than a 44-page DID. Include intended government TDP use cases in the RFP (as done by the Army Future Long Range Assault Aircraft) so the proposal can offer appropriate deliverables and data rights. Consider Data Escrow, with specified trigger events, to hedge against emergency use needs or loss of the original supplier. Allow spare parts bidders to negotiate use of IP directly with original manufacturers rather than relying on DoD TDPs. For software and firmware, use the commercial practice of Application Program Interfaces (APIs) rather than requiring source code.
- User Story 49: Update MIL-STD-31000 to include the minimum data needed for additive manufacturing. Build a centralized system for managing technical data packages (TDPs)

with version control, real-time updates, and integration with Additive Manufacturing (AM) platforms. Develop a database for AM material properties, tolerances, and stress thresholds specific to depot operations. Partner with manufacturers to enrich the database with certified material data. Use digital twins to simulate and test parts before fabrication and incorporate real-time feedback from digital twins to improve part accuracy and quality. Define and implement standards for data formats to ensure compatibility across all AM systems. Develop secure APIs for (1) seamless data exchange between depots and external suppliers, and (2) software/firmware associated with replacement parts to eliminate need for source code.

- User Story 47: Incorporate all these ideas into a future target called Technical Data as a Service (TDaaS). The TDaaS concept was well defined in a Naval Postgraduate School paper, "Technical Data as a Service (TDaaS) and the Valuation of Data Options" (Thompson & McGrath, 2019). Workshop participants agreed that the issues and ideas from the other TDP-related user stories could fit within the TDaaS framework, with centralized access to data (through PLM or other systems) as a near term implementation target and distributed access to data at its source as a longer-term target.

IDMP Roadmap

Post processing of the workshop results developed specific IDMP roadmaps for each user story and an overall roadmap for migration to the TDaaS concept (see Figure 3).

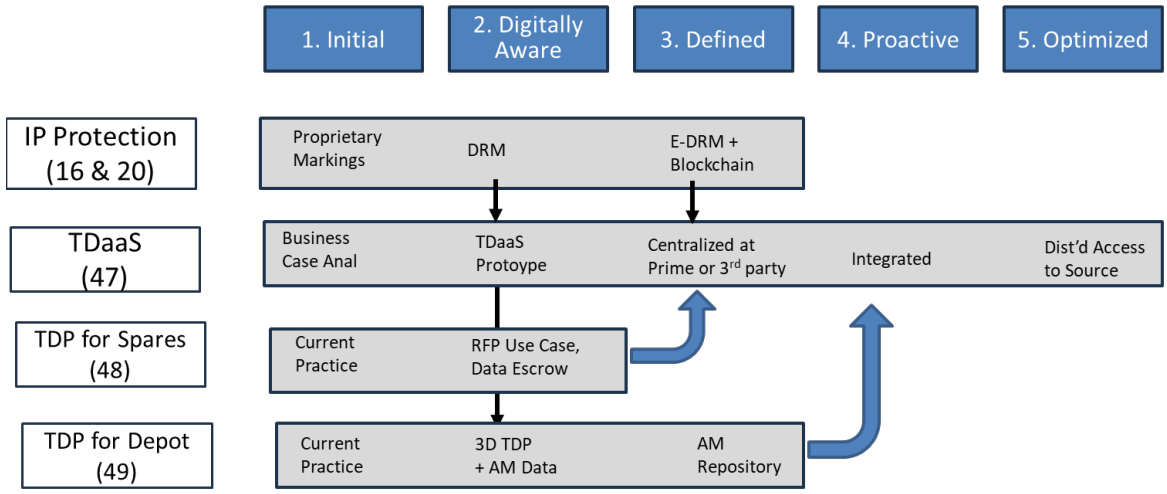

Figure 3: TDaaS Could Become the Target for Higher Maturity Levels

The NDIA DMWG is discussing this roadmap and the workshop ideas with government stakeholders to determine which ideas are ready for implementation and which need further demonstration and prototyping to resolve technical and business process uncertainties.

Findings

The findings of this research provide insights into the applicability of the Integrated Digital Maturity Pathway (IDMP) in addressing challenges associated with Technical Data Packages (TDPs), interoperability, and intellectual property (IP) protection within the Department of Defense (DoD) acquisition framework. Through an extensive analysis of case studies, working group discussions, and user story development, the research highlights three

key areas of improvement: enhanced TDP practices, validation of the IDMP framework, and its broader applicability to digital transformation initiatives.

Enhanced TDP Practices

One of the most significant findings from this study is the need for improved TDP practices to facilitate DoD sustainment and acquisition. The Digital Manufacturing Working Group (DMWG) identified that current TDPs often suffer from incomplete documentation, lack of interoperability, and outdated technical data (DMWG, 2024). The analysis revealed that contractors frequently limit access to proprietary data due to IP concerns, forcing the DoD to negotiate for TDPs at various points in the product life cycle, often at higher costs and under restrictive conditions.

Findings from workshop discussions and user story development indicate that digital transformation, guided by the IDMP framework, can significantly improve TDP accessibility. The incorporation of secure digital rights management (DRM), blockchain verification, and structured data-sharing protocols allows for better protection of contractor IP while ensuring sufficient data availability for DoD sustainment and modernization efforts. Additionally, findings highlight the viability of a Tech Data as a Service (TDaaS) model, which shifts away from traditional upfront TDP acquisition toward a subscription-based access model that ensures the availability of up-to-date and relevant technical data as needed.

Validation of the IDMP Framework

The study validates the IDMP framework as an effective model for guiding digital maturity across government, contractors, and defense supply chain partners. Through its structured maturity levels, IDMP enables progressive digital transformation, allowing organizations to assess and enhance their technical data management capabilities. Case study findings show that IDMP's structured approach to interoperability, data governance, and security improves digital transformation efforts by addressing specific gaps in data-sharing policies and IP protections.

A key aspect of this validation is the role of user stories in shaping the IDMP framework. Monthly workgroup meetings generated 80 user stories, which were analyzed to identify common challenges in TDP management, digital rights, and additive manufacturing.

The application of user stories provided a direct mechanism for capturing stakeholder needs and aligning them with IDMP principles, reinforcing the practicality and scalability of the framework.

Broader Applicability of the IDMP Framework

The findings suggest that the IDMP framework has broad applicability beyond TDP management, extending to other areas of digital transformation within the defense industrial base. Case studies highlight its relevance in addressing challenges related to digital twins, data analytics for Industry 4.0, and configuration management. The analysis of user stories and working group discussions supports the scalability of IDMP to additional defense acquisition challenges, reinforcing its potential as a foundational framework for DoD digital modernization.

Additionally, the research identifies the importance of integrating emerging technologies such as AI, machine learning, and blockchain to further enhance digital maturity and sustainment capabilities. Applying IDMP principles to advanced manufacturing, predictive maintenance, and secure data exchange, the DoD and its industrial partners can create a more resilient, interoperable, and future-ready digital ecosystem.

Conclusion

The study's findings underscore the critical role of IDMP in transforming DoD technical data practices, validating its effectiveness in improving TDP accessibility, protecting contractor IP, and enabling scalable digital transformation efforts. The use of case studies and user stories demonstrates the practical applicability of the framework, while the integration of VAULTIS principles reinforces its alignment with broader DoD digital strategy initiatives. Furthermore, the research highlights the IDMP framework's potential for broader adoption, positioning it as a key enabler of future defense acquisition modernization efforts.

References

Al Shidhani, A. A. (2019). Cyber defense maturity levels and threat models for smart cities. *International Journal of Information Security and Privacy*, *13*(2), 32–46. https://doi.org/10.4018/IJISP.2019040103

Bertuca, T., & Judson, J. (2012). Legislation at play: Technical data package purchases re-emerge as important issue for Army. *Inside the Pentagon's Inside the Army*, *24*(14), 1–9.

Cohn, M. (2004). *User stories applied: For agile software development*. Addison-Wesley.

Department of Defense. (2018). *MIL-STD-31000B, Technical data packages*. http://everyspec.com/MIL-STD/MIL-STD-10000-and-Up/download.php?spec=MIL-STD-31000B.055788.pdf

Domnik, J., & Holland, A. (2024). On data leakage prevention maturity: Adapting the C2M2 framework. *Journal of Cybersecurity and Privacy*, *4*(2), 167–195. https://doi.org/10.3390/jcp4020009

Harper, J. (2017). Should *project managers buy technical data* (DTIC Technical Reports, AD1040333).

Kekeya, J. (2021). Qualitative case study research design: The commonalities and differences between collective, intrinsic and instrumental case studies. *Contemporary PNG Studies*, *36*, 28–37.

Kırmızı, M., & Kocaoglu, B. (2022). Digital transformation maturity model development framework based on design science: Case studies in manufacturing industry. *Journal of Manufacturing Technology Management*, *33*(7), 1319–1346. https://doi.org/10.1108/JMTM-11-2021-0476

Kuusisto, O., Kääriäinen, J., Hänninen, K., & Saarela, M. (2021). Towards a micro-enterprise–focused digital maturity framework. *International Journal of Innovation in the Digital Economy*, *12*(1), 72–85. https://doi.org/10.4018/IJIDE.2021010105

Lucassen, G., Dalpiaz, F., van der Werf, J. M. E. M., & Brinkkemper, S. (2016). Forging high-quality user stories: Towards a discipline for agile requirements. *Proceedings of the IEEE 24th International Requirements Engineering Conference (RE'16)*, 126–135.

Lucassen, G., Robeer, M., Dalpiaz, F., van der Werf, J. M. E. M., & Brinkkemper, S. (2017). Extracting conceptual models from user stories with Visual Narrator. *Requirements Engineering*, *22*(3), 339–358. https://doi.org/10.1007/s00766-017-0270-1

McKay, A., Rice, H. P., Chau, H. H., & de Pennington, A. (2021). *Maintaining consistency across design descriptions in engineering product development*. Cambridge University Press. https://doi.org/10.1017/pds.2021.460

Moon, L. , Clancy, G. , Welton, J. & Harper, E. (2019). Nursing value user stories. *Computers, Informatics, Nursing*, *37*(3), 161–170. https://doi.org/10.1097/CIN.0000000000000520

Poderi, G., Hasselqvist, H., Capaccioli, A., Bogdan, C., & D'Andrea, V. (2020). Matters of concerns and user stories: Ontological and methodological considerations for collaborative design processes. *CoDesign*, *16*(3), 220–232. https://doi.org/10.1080/15710882.2018.1557694

Ridder, H.-G. (2017). The theory contribution of case study research designs. *Business Research (Göttingen)*, *10*(2), 281–305. https://doi.org/10.1007/s40685-017-0045-z

Ross, N. J. (2015). Technical data packages: When can they reduce costs for the Department of Defense? *Defense AR Journal*, *22*(4), 450–471.

Shepherd, A. (2024). *Navy gains more access to F/A-18 technical data*. InsideDefense.Com's SitRep, http://proxy.lib.odu.edu/login?url=https://www.proquest.com/trade-journals/navy-gains-more-access-f-18-technical-data/docview/3031700409/se-2

Shepherd, A. (2024). Super Hornet technical data package access will allow Navy to be self-sufficient. *Inside the Pentagon's Inside the Navy*, *37*(32), http://proxy.lib.odu.edu/login?url=https://www.proquest.com/trade-journals/super-hornet-technical-data-package-access-will/docview/3091582955/se-2

Thompson, G. E., & McGrath, M. (2019). *Technical data as a service (TDaaS) and the valuation of data options*. Acquisition Research Program. https://dair.nps.edu/handle/123456789/2757

Vera-Rivera, F. H., Puerto Cuadros, E. G., Perez, B., Astudillo, H., & Gaona, C. (2023). SEMGROMI-a semantic grouping algorithm to identifying microservices using semantic similarity of user stories. *PeerJ. Computer Science*, *9*, e1380–e1380. https://doi.org/10.7717/peerj-cs.1380

Wautelet, Y., Heng, S., Kiv, S., & Kolp, M. (2017). User-story driven development of multi-agent systems: A process fragment for agile methods. *Computer Languages, Systems & Structures*, *50*, 159–176.

Wesley, R. D. (2021). Innovation at Mach5. *Army AL & T*, 37–42. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/trade-journals/innovation-at-mach5/docview/2488113752/se-2

Wilson, N. (2023). USMC considers Add'l ACV maker, lacks technical data package rights. *Inside the Pentagon's Inside the Navy*, *36*(19). http://proxy.lib.odu.edu/login?url=https://www.proquest.com/trade-journals/usmc-considers-addl-acv-maker-lacks-technical/docview/2813539993/se-2

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net