Enabling a Sharing Economy to Accelerate Change in Immersive Training

Krissa Watry, Christina Padron, Victoria Claypoole, Stephen Hopp
Dynepic, Inc.
Reno, Nevada
Krissa; Christina; Victoria; Stephen {@dynepic.com}

Margaret Merkle
USAF AFLCMC WNS
Dayton, Ohio
margaret.merkle.1@us.af.mil

ABSTRACT

Training and simulation products developed and deployed for the government should target a common operating environment that expects compatibility, interactivity, and security. Diverse training application and content developers generally do not create standardized or interoperable software environments, leaving large organizations with stove-piped content that is challenging to integrate and manage. New models of continuous integration/continuous deployment environments, such as the USAF Platform One, establish unified delivery spaces for software applications, but do not yet support a unified training ecosystem for specialized content sharing. Building virtual, augmented, and mixed reality (extended reality, or XR, collectively) training systems, training content, and enabling technologies using a modular open systems approach (MOSA), provides the opportunity for a central hub which allows discovery, distribution, and reuse of different types of digital assets (e.g., XR applications, lessons, 3D models, AI/ML models, assessment tools, visualization tools). Enabling a hub to support a sharing economy featuring digital asset contributors, builds an organized, democratized process to revolutionize training systems.

There are still process, programmatic, and contractual challenges and considerations, including how to define who can access, share, re-use, and modify assets, and how author credit designation and/or license fees might be handled. Ensuring that a central hub respects data rights, incentivizes contributors, and fuels a collaborative ecosystem is imperative. Additional challenges include how to control asset permissions on de-centralized repository content and enable discoverability via the central hub. This paper describes the design, development, and instantiation of a centralized hub for the discovery and distribution of immersive, XR training technologies. The methodology for overcoming some of the challenges is discussed, with preliminary results from several pilot programs with over 30 individual third-party training application vendors. Finally, the paper concludes with a discussion of lessons learned and future considerations for leveraging a centralized hub to accelerate change in immersive learning.

ABOUT THE AUTHORS

Ms. Krissa Watry is Co-Founder and CEO of Dynepic, Inc. As a Captain in the USAF, Krissa was the Chief Engineer for Milstar at 4th Space Operations Squadron managing the operations of the ultra-secure communication satellite constellation in GEO. Krissa spent over 10 years designing, building, launching and operating cutting-edge space systems for organizations like NASA, DoD, and others, including spaceflight hardware that docked with the International Space Station. In addition, Krissa is a multi-preneur with over 10 years as a technology executive who has founded multiple companies and commercialized a multitude of hardware and software products across the sports, education, kids and family, and defense industries. Krissa holds 10 patents and is recognized as a Global Innovator and Entrepreneur by President Obama. She holds a BS in Engineering Mechanics from the US Air Force Academy, and was a Draper Laboratory Fellow achieving a MS in Mechanical Engineering from MIT focused in product design.

Ms. Christina Padron is the Vice President of Partnerships and Growth at Dynepic, Inc. She is an experienced Principal Investigator, program manager, researcher, and human factors engineer with over 15 years of experience in managing the design, development and evaluation of virtual assessment and training tools for a variety of military research organizations. Christina is responsible for leadership of strategic partnerships that facilitate the Dynepic ecosystem of integrated training and operational products, as well as leadership over Dynepic's growth opportunities. She holds an MS from Penn State University in Industrial Engineering, and a BS from Purdue University in Industrial Engineering**.**

Dr. Victoria Claypoole is currently the Manager of New Horizons at Dynepic, Inc. With previous experience at the Air Force Research Lab and her current work with various DoD agencies, Dr. Claypoole's research interest lies at the intersection of increasing warfighter readiness and advancing scientific knowledge. Dr. Claypoole has earned numerous professional awards, including the University of Florida's 40 under 40, the University of Central Florida's 30 under 30, and several Best Paper awards at various conferences. She received a Ph.D. in Human Factors and Cognitive Psychology and a Master's in Modeling and Simulation from the University of Central Florida.

Mr. Stephen Hopp is the Director of Programs at Dynepic, Inc. He is an experienced program management professional, systems engineer and leader with over 30 years of military and industry experience. During his 24-year Air Force career, he supported six different Air Force Major Commands in roles ranging from Satellite Engineer; Intelligence, Surveillance and Reconnaissance Engineering Analyst; Global Hawk Acquisition and Requirements Liaison, and AFROTC Instructor. As government civilian, he worked on the T-X (now designated as the T-7A) acquisition program as the Lead Engineer for the T-7A Maintenance Training System. He holds a BS in Electrical Engineering from the University of Colorado at Colorado Springs, and MS in Electrical Engineering from the Air Force Institute of Technology.

Ms. Margaret Merkle is Innovation Technology Chief, Simulators Division, Agile Combat Support Directorate, Air Force Life Cycle Management Center at Wright-Patterson AFB Ohio. She is responsible for leading the exploration, prototyping and integration of novel technologies into aircrew training and simulation systems, overseeing Pitch Day competitions and other innovation and research projects. She holds a Bachelor of Science in Business Administration in Management Information Systems and International Business from Bowling Green State University, and a Master of Business Administration from the University of Dayton.

Enabling a Sharing Economy to Accelerate Change in Immersive Training

Krissa Watry, Christina Padron, Victoria Claypoole, Stephen Hopp
Dynepic, Inc.
Reno, Nevada
Krissa; Christina; Victoria; Stephen {@dynepic.com}

Margaret Merkle
USAF AFLCMC WNS
Dayton, OH
margaret.merkle.1@us.af.mil

INTRODUCTION

High fidelity training has long been critical to ensuring the readiness of U.S. Warfighters, particularly to supplement training for those positions in which live training is high-risk and requires expensive resources to conduct (e.g., pilot training; Champney et al., 2017). However, high fidelity training simulators have traditionally been developed as closed systems. To overcome some of these challenges, training developers have looked towards “lightweight simulators”, or virtual, augmented, and mixed reality (extended reality, or XR, collectively) training systems. However, even these tend to be developed in a silo and are not interoperable with other operating systems. Therefore, the U.S. Government is interested in building the training systems of the future with a Modular Open Systems Approach (MOSA), made of integrated training technologies and content that are easily accessed, updated, and shared.

MOSA is US Law (10 USC 4401); specifically, that “A major defense acquisition program that receives Milestone A or Milestone B approval after January 1, 2019, shall be designed and developed, to the maximum extent practicable, with a modular open system approach to enable incremental development and enhance competition, innovation, and interoperability. Other defense acquisition programs shall also be designed and developed, to the maximum extent practicable, with a modular open system approach to enable incremental development and enhance competition, innovation, and interoperability” (10 USC 4401). Put simply, MOSA requires modular and integrated system interfaces between major systems, subsystems, and components and other modular systems.

In this vein, training and simulation products developed and deployed for the government should target a common operating environment that provides the infrastructure for compatibility, interactivity, and security. Training systems must be compatible wherein multiple systems can exist together under one training program umbrella without issue. Similarly, training systems must allow interactivity so that data can securely be passed back and forth between systems; closed, proprietary data sources must not hinder the MOSA. Finally, training systems must have strict security rules; a MOSA does not necessarily mean open source, which can introduce security vulnerabilities. MOSA-based training systems must ensure security is maintained and reduce vulnerabilities.

To overcome these initial challenges, the U.S. Government has funded several continuous integration/continuous deployment (CI/CD) environments, such as the U.S. Air Force’s Platform One, to establish and enable unified delivery spaces for software applications. However, these new CI/CD environments do not yet support a unified training ecosystem for specialized content development, such as that required for extended reality (XR, e.g., augmented and virtual reality) training systems. For example, while existing CI/CD pipelines are ideal for simple applications that want to get up and running quickly, they are not suitable for complex systems that have shared assets and services (Watry, Padron, & Merkle, 2021). They also fail to meet the unique requirements of XR, such as streaming and XR device support. Additionally, due to XR’s “lightweight nature”, most XR training systems can live in a cloud environment and be accessed from a single, centralized interface (or marketplace hub approach) – even when the XR training systems span multiple major systems, when built using MOSA guidelines.

XR training systems, training content, and enabling technologies are generally being developed on a handful of gaming engines, which supports efficiencies in the reuse of different levels of digital assets across training – from 3D models, environments, and other assets to full lessons and experiences. Further, agnostic training tools such as Artificial Intelligence (AI) models, virtual instructors, and evaluation tools, can be applied across different training scenarios and systems. However, this requires a sharing economy across vendors and government in the training ecosystem. This paper will discuss a concept for the implementation of a sharing economy currently under development to solve some of these challenges that utilizes a central hub platform built with a MOSA that has open Application Programming Interfaces (APIs) and Software Development Kits (SDKs) to power third party digital assets of all different types. This implementation is undergoing preliminary prototyping and testing, and some of the results and lessons learned to this point will be shared.

ENABLING A SHARING ECONOMY

A sharing economy is enabled by the collaborative consumption through sharing, exchanging, and selling goods and services (Pushmann & Alt, 2016). Sharing economies are typically facilitated through digital platforms and enable community, access, and collaboration in the sharing, purchasing, and selling of goods/services (Richardson, 2015). It has also been defined as ‘online platforms that help people share access to assets, resources, time, and skills’ (Wosskow, 2014). The exact definition of a sharing economy is varied throughout the literature (e.g., Hossain, 2020; Richardson, 2015; Puschmann & Alt, 2016), however, most definitions tend to converge around the concept of sharing assets in such a way that introduces efficiency and sustainability and bringing opportunities to new businesses.

There are many realized benefits of sharing economies; particularly that those who engage in sharing economy experience time saved, reduced costs (both near-term and long-term), and a commitment to social transformation through values of sharing and collaboration (Curtis & Lehner, 2019). Other benefits include the opportunity to generate revenue through the sharing economy platform (Heo, 2016), reduce resource use and potential waste (Heinrichs, 2013), enable economic growth that is sustainable (Bonciu & Balhar, 2016), and ultimately, convenience (Curtis & Lehner, 2019).

Many sectors, such as content streaming, travel, and car sharing, have leveraged sharing economies with great success. Interestingly, start-up companies and small businesses represent a significant percentage of innovation within sharing economies (Koetsier, 2015) – which is promising for a government sharing economy wherein the introduction and success of non-traditional defense contractors can be realized.

Some prominent examples of sharing economies in the commercial sector include Amazon, Envato Elements, Sketchfab, YouTube, Roblox, GitHub, and Thingiverse. For example, Thingiverse allows users to upload CAD models for 3D printing onto their hub/marketplace. Other users can download, use, modify and re-list these assets to contribute to the growing open ecosystem. Thingiverse operates in a generally free market wherein the designs and models are licensed under Creative Commons or General Public licenses. While Thingiverse is primarily free and open to everyone, other sharing economies operate on more of a permissions-based framework that can limit access. For example, GitHub is a sharing economy for source code development. Code can be openly shared or locked down behind a permissions-based framework wherein the developer can choose who can access and modify the original code. Code that is open enables other developers to build off the original code and enhance and further the code capabilities. In each example, a collaborative ecosystem is present wherein users can contribute and grow the knowledge base while simultaneously saving time and development re-work. Each of these sharing economies faces specific challenges to development and facilitation, including various technical challenges of supporting diverse platforms and technologies, along with enticing users to contribute.

Building a sharing economy is challenging in the commercial sector. However, the unique constraints of the US Government can make it even more challenging to build a burgeoning sharing economy for next-gen training.

Examples of these challenges include:

1) the digital asset rights, permissions, and licenses are not always clearly defined or readily accessible outside the contract;
2) there is no central digital asset library that enables the reuse of digital assets;
3) there is a lack of a structure and process to capture the rights, permissions, and licenses to effectively implement a central digital asset library;
4) external repositories need to be able to publish permissions and asset listings, so they are discoverable via a central hub;
5) streamlined mechanisms for enabling contracting for/payment for the use of licensed digital assets are needed; and
6) US Government security controls and labeling requirements must be adhered to and maintained.

Despite these challenges, the positive impact of implementing a sharing economy for next-gen training could be immense, as a centralized sharing hub will accelerate innovation and enable organic change as technology mission needs evolve.

Initial Considerations for a Sharing Economy

There are quite a few considerations in the development and facilitation of a sharing economy, especially one funded by the U.S. Government. As these considerations were defined, they were categorized into the following: Technical and Process Considerations. Though not an exhaustive list, some of the major considerations are described in the sections below.

Technical Considerations

For a sharing economy to work, it is critical that the disparate technologies can integrate seamlessly with each other from a technical perspective. There must be infrastructure and standards that support communication between all the disparate software, hardware, AI, sensors, etc. It is important for the ecosystem to remain as hardware and software agnostic as possible. One consideration from the infrastructure perspective is whether to use a centralized hub or a federated network.

When looking at network architecture types, most networks are centralized, distributed, or decentralized (Poenitzsch, 2018). A centralized network enables all data sources to push and pull data from a centralized node; there is a central organization point and centralized decision making. A distributed network contains no central node, instead, the data sources push and pull their data from interconnected data streams, no single entity controls information flow. Finally, a decentralized network is a combination of the previous two wherein multiple centralized networks are connected through a distributed network – meaning that though there may be a centralized node, there is no single node that controls the network.

Both distributed and decentralized networks are federated networks; importantly, a centralized network cannot be federated by nature, as federated is defined as non-centralized. Federated networks allow groups of interconnected networks to push and pull data between parties; each party is interconnected to one another (VMWare, 2022). A federated network ultimately allows multiple networks to work together and function as one. In a federated network, there is no central service to connect to directly; instead, the network is comprised of an organized mesh of nodes that are all interconnected. In the case of a sharing economy, every participant in the sharing economy would have to connect with one another. This could cause potential data losses if one of the participants were removed from the sharing economy, and potentially violate MOSA principles.

On the other hand, a centralized network is more like a hub and spoke wherein there is one centralized access point, and all the data sources connect in to this one spot. The centralized hub allows for efficiency when managing standards, communications, and security requirements. It also leads to savings on costs, as centralized services can be shared across the network without introducing redundancy (e.g., the hub provides a central permission wizard for tagging content with a common standard for asset tagging and access permissions). Within the centralized hub model, sharing economy participants must communicate with the government's central authority to communicate with each other. This would provide the government with more control over the sharing economy standards and ensure a modular approach (e.g., removing one participant from the sharing economy does not disrupt the other connections). Because of its modularity, it would be easy to remove (or add) training systems and applications from the sharing economy without needing to replicate services or connections the way one would in a federated network. Finally, a central hub was also chosen over a federated network due to the permissions and identity management needed for a sharing economy. A central hub that controls identity and permission management is ideally suited for data management standards. Overall, this approach would minimize redundancy, reduce costs, ensure interoperability, reduce potential for exposure of security vulnerabilities, and allow the government more control over the sharing economy.

Process Considerations

There are also a variety of process considerations in the execution of a successful sharing economy in the U.S. Government. For example, determining the process for an accelerating Authority to Operate (ATO) and other certifications for all of the technologies included in the sharing economy. There are always challenges that occur with obtaining an ATO for a new system or platform, and for a platform attempting to foster a shared economy it is even more true. For example, one challenge is attempting to determine which assets and applications can be hosted as "content" within the centralized hub's authorization boundary where they do not need their own ATO, and whether they require a full Assess and Authorize (A&A) effort or an Assess Only, as described in AF Instruction 17-701 (Kelly, 2019). Adding to this challenge is the inclusion of peripheral devices into the sharing economy boundary that display the training content / applications. There currently are no security technical implementation guidelines (STIGs) or security requirements guides (SRGs) associated with XR technologies or the peripheral devices commonly used to support XR content.

Additionally, consideration of the sharing economy is how permissions are implemented across the ecosystem of technologies. To facilitate a sharing economy, the central hub needs to ensure that, where appropriate, Intellectual Property (IP) and data rights associated with content provided under contractual agreements are respected and protected, the government's content is labeled with proper classification and distributed appropriately, and where appropriate, vendor's content is further protected according to open sharing licenses like Creative Commons. To do so, defining the terminology associated with the data rights, classification, distribution statements or limited distribution controls (LDC), and Creative Commons leads to defining variations of access and usability. Other key considerations are the classification of the content, if it has been approved by the military organization's Public Affairs Office, and when applicable, the Foreign Disclosure Office. All these factors and considerations must be accounted for to assign the permissions needed to facilitate a sharing economy. Further, the hub must correlate those considerations to assigned permissions, and support "orphaned" technologies. The development of a permissions framework to enable a sharing economy is the key focus of this paper.

DEVELOPMENT OF A SHARING ECONOMY

To develop and instantiate a true sharing economy, it was first determined that a central hub for discovery and distribution of the technologies must exist. The central Hub was chosen instead of a federated network because of the immense benefits, such as cost savings, reduction in redundancy, interoperability, and modular configurations that provide the government the most control over the sharing economy.

The Hub provides an open ecosystem of technologies that are integrated through a platform interface. The platform was built with a MOSA principles, embracing an open architecture to support many content creators, that ultimately leverages a privacy-secure framework with a zero-trust architecture for ecosystem applications. According to SP 800-207, Zero Trust Architecture, "Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)."

The Hub provides a secure marketplace for the discovery of DoD training content creators' and third-party vendors' 3d models, lessons, experiences, and applications. The Hub facilitates the government's sharing economy as it enables the discovery, distribution, and use of training applications. Because of its MOSA architecture, the Hub can connect to existing DoD systems to facilitate the data exchange between official DoD systems and third-party vendors in the pursuit of enhancing current DoD training. With the centralized Hub, content contributors can list items on the platform making them available for use within the sharing economy. Note that the terms "content" and "content contributions" are used broadly; content can mean any type of community listing such as a training scenario, training vignette, complete training lesson, AI agent, 3D models, PDF, Slide Deck, Map Pack, Plugin, Smart Scene, XR training program, XR self-authoring tool, training application, etc.

Once the infrastructure of the Hub was determined, the next consideration to work through – and the focus of this paper – was to determine how rights and permissions were handled in the central digital asset library of the Hub. This component is integral to the success of the sharing economy, as it ensures that participants are protected from loss of IP and that they feel comfortable with contributing to the sharing economy.

Methodology for a Permissions Framework

To ensure participation of DoD and third-party organizations within a single sharing economy, the centralized Hub that hosts the applications and resulting training content must accurately and appropriately protect IP and data rights. To address this problem, a framework for permissions was developed that leverages current government processes and a common commercial approach– distribution statements, data rights, and creative commons. There are three integral components associated with determining permissions within a sharing economy:

1. Identify and define the different influences on content permissions and how permissions are defined today
2. Identify the different types or levels of allowable content interactions – what can participants do with the content?
3. Identify the process to determine user's ability to access, share, re-use, and modify content based on the content's attributes and user access permissions (data rights or Creative Commons, distribution statements, classification, etc.)

Factors Influencing Content Permissions and How Permissions are Defined

By looking at the various methods by which permissions are defined, the factors were narrowed down to take into consideration Data Rights associated with contractual agreements (DFARS 252.227-7017; Defense Information Systems Agency, 2021), the DoD's Distribution Statements (DoDI 52230.24), and Creative Commons Licenses (Creative Commons Corporation, 2020; 2021; 2022). The DFARS, Distribution Statements and CCLs are different existing ways to describe and categorize content, and are useful, and even required means of labeling content. These guidelines helped determine *who* could interact with the content / applications within the sharing economy and exactly *what* level of interaction was permitted. In this paper, we seek to use these categories, not to change or improve them, that is beyond the scope of this effort.

Data Rights were defined based off the chart in Table 1. According to Defense Acquisition University, Data Rights are "Government's legal license right to use, modify, reproduce, perform, display, release or disclose the noncommercial technical data or noncommercial computer Software" (DFARS 252.227-7017). Data rights are determined by a number of factors including who paid for the technical development of the data or computer software. Data rights are typically negotiated between the contractor and the government agency. Data rights determine *who and how a user* can interact with the content / application. For the current permissions framework, data rights were used as the starting point for determining the matrix of permission availability. While traditionally data rights are asserted at various level of code (i.e., source, object, executable), the data rights incorporated for the permissions framework were only concerned with data rights at the level of the content being shared.

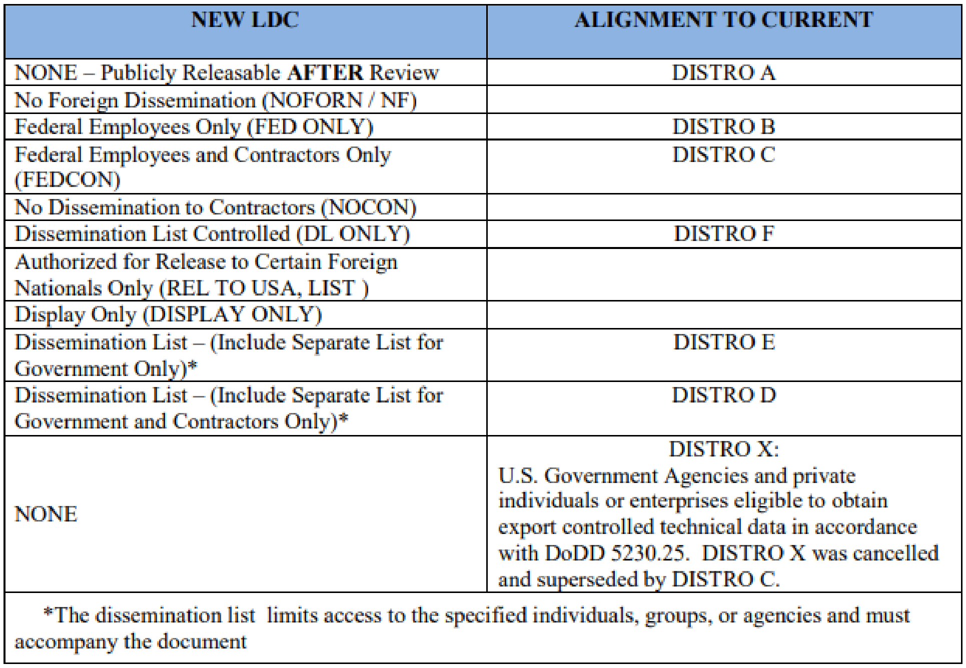
Table 1. Definition of Data Rights

Rights Category	Applies to these Types of Technical Data (TD) or Computer Software (CS)	Rights Criteria	Permitted Uses with the Government	Permitted Uses by Third Parties Outside the Government
Unlimited Rights (UR)	Noncommercial TD and CS	Developed exclusively at Government expense, and certain types of data (e.g., Form, Fit, and Function data [FFF]; Operation, Maintenance, Installation, and Training [OMIT]).	All uses; no restrictions	
Government Purpose Rights (GPR)	Noncommercial TD and CS	Developed with mixed funding	All uses; no restrictions	For "Government Purposes" only; no commercial use
Limited Rights (LR)	Noncommercial TD Only	Developed exclusively at private expense	Unlimited; except may not be used to manufacture	Emergency repair or overhaul
Restricted Rights (RR)	Noncommercial CS Only	Developed exclusively at private expense	Only one computer at a time; minimum backup copies; modification	Emergency repair/overhaul; certain services/maintenance contracts
Specifically Negotiated License Rights	Any/all TD and CS – including commercial TD and CS	Mutual agreement of the parties; use whenever the standard categories do not meet both parties' needs	As negotiated by the parties; however, must not be less than LR in noncommercial TD and must not be less than RR in noncommercial CS	
Small Business Innovative Research (SBIR) Data Rights	Noncommercial TD and CS	All TD or CS generated under a SBIR contract	The equivalent of UR in OMIT and FFF data; the equivalent of LR in all other delivered TD; the equivalent of RR in CS	
Commercial TD License Rights	Commercial TD Only	TD related to commercial items (developed exclusively at private expense)	The equivalent of UR in OMIT and FFF data; the equivalent of LR in all other delivered TD	
Commercial CS Licenses	Commercial CS Only	Any commercial CS or CS documentation	As specified in the commercial license customarily offered to the public	

Considered next were the DoD's Distribution Statements. Because the Hub can list and distribute any type of content, including technical data, for use within the sharing economy, *and* sharing economy participants can span robust user types (e.g., government personnel, government contractor, industry partner, foreign nationals, etc.), it was critical to take into account specific DoD distribution statements to ensure Controlled Unclassified Information (CUI) and non-CUI data was appropriately protected. Document control guidance is provided for the Distribution Statements shown in Table 2 (DoDI 52230.24) for non-CUI or Limited Dissemination Control if CUI (Figure 1). To fully support these controls, the Hub and its platform interface must have extensive knowledge of the participant's profile in order to adequately assign permissions based on the DoD distribution statements. Distribution statements help further delineate *who* can interact with the items within the sharing economy. These classifications were included within the permissions framework matrix in addition to the data rights described above.

Table 2. Definitions of Distribution Statements

Distribution Statement	***Description***
Distribution Statement A	Approved for public release: distribution unlimited.
Distribution Statement B	Distribution authorized to U.S. Government agencies.
Distribution Statement C	Distribution authorized to U.S. Government agencies and their contractors.
Distribution Statement D	Distribution authorized to Department of Defense and U.S DoD contractors.
Distribution Statement E	Distribution authorized to Department of Defense.
Distribution Statement F	Further dissemination only as directed.



NEW LDC	ALIGNMENT TO CURRENT
NONE – Publicly Releasable **AFTER** Review	DISTRO A
No Foreign Dissemination (NOFORN / NF)	
Federal Employees Only (FED ONLY)	DISTRO B
Federal Employees and Contractors Only (FEDCON)	DISTRO C
No Dissemination to Contractors (NOCON)	
Dissemination List Controlled (DL ONLY)	DISTRO F
Authorized for Release to Certain Foreign Nationals Only (REL TO USA, LIST)	
Display Only (DISPLAY ONLY)	
Dissemination List – (Include Separate List for Government Only)*	DISTRO E
Dissemination List – (Include Separate List for Government and Contractors Only)*	DISTRO D
NONE	DISTRO X: U.S. Government Agencies and private individuals or enterprises eligible to obtain export controlled technical data in accordance with DoDD 5230.25. DISTRO X was cancelled and superseded by DISTRO C.

*The dissemination list limits access to the specified individuals, groups, or agencies and must accompany the document

Figure 1. Limited Dissemination Control (LDC) alignment to Distribution Statements.

Finally, Creative Commons licenses provide a consistent and standardized way to afford public permission of creative work in accordance with copyright law. Creative Commons licenses provide the public with information on what, specifically, they can do with any relative work. Creative Commons distinguishes between six different license types – all with varying degrees of permissiveness (see Table 3). Creative Commons specify *what* can be done with the content, more-so than *who can do what* with the content – as is found within Data Rights and DoD Distribution Statements. These statements were rolled into the permissions framework and leveraged to determine exactly what interactions were permissible with content found within the sharing economy (described in more detail in the next section).

Table 3. Descriptions of Creative Commons Licenses

CC License Type	*Definition*
CC0 (CC Zero)	CC0 (aka CC Zero) is a public dedication tool, which allows creators to give up their copyright and put their works into the worldwide public domain. CC0 allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, with no conditions.
CC BY	This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use.
CC BY-SA	This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use. If you remix, adapt, or build upon the material, you must license the modified material under identical terms.
CC BY-NC	This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format for noncommercial purposes only, and only so long as attribution is given to the creator.
CC BY-NC-SA	This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format for noncommercial purposes only, and only so long as attribution is given to the creator. If you remix, adapt, or build upon the material, you must license the modified material under identical terms.
CY BY-ND	This license allows reusers to copy and distribute the material in any medium or format in unadapted form only, and only so long as attribution is given to the creator. The license allows for commercial use.
CC BY-NC-ND	This license allows reusers to copy and distribute the material in any medium or format in unadapted form only, for noncommercial purposes only, and only so long as attribution is given to the creator.

Identification of Different Types of Allowable Content Interaction

The next component to determine was what exactly could participants in a sharing economy do with the listings that were available to them. The process to identify the different types or levels of allowable content interaction started with those identified by Creative Commons. Creative Commons categorizes different interaction types as the user’s ability to distribute, remix, adapt, and build upon content in the ecosystem. After several iterations and consideration of the various origins of the permissions, users’ ability to access, share, re-use, and modify content set the foundation for content interaction, a mapping of Creative Commons to the sharing economy users’ permissions was achieved. The final definitions of permissible user interactions within the sharing economy are delineated in Table 4. Overall, it was determined that contributors could set specific permissions that allow other users to either discover, download, use, distribute, or modify/remix their listings within the sharing economy. Importantly, the “discover” interaction is meant to provide deep protection for the sharing economy. For example, a large organization may list content that contains IP that they do not want other participants seeing; in this example, they can revoke the “discover permission”, resulting in that specific listing being undiscoverable for certain user types. Similarly, a DoD organization may be listing technical data that is CUI. In this case, the “Discover” interaction would prevent users who do not have the proper credentials from viewing the listing. Additionally, the allowed user interaction levels include the preceding levels. For instance, if a user could ‘use’ content, they would by default be able to Download and Discover that content, but not Distribute or Modify/Remix.

Once the variables were defined, the next step was to determine how permissions could and should impact the discoverability and access of all content within the ecosystem. This process presented a complex puzzle. The numerous factors that needed to be accounted for added to complexity. Given that content created by vendors may have associated Data Rights, as defined by their contractual agreement(s) with the government, and that some content could have Distribution Statements or Limited Dissemination Controls assigned by the designated government authority (indicating that the information is Controlled Unclassified Information), and that some vendors may provide content through their own initiative, in which case Creative Commons standards may apply, there were many variables that could impact the permissions assigned to content. Add in government Public Affairs approval for public release, and releasability tagging for foreign government personnel, and the complexity grew.

Table 4. Definitions of User Interactions within Sharing Economy

Breakdown	*Description*
Discover	Discover permissions allow users to view the listing details page.
Download	Download permissions allow users to download a listing.
Use	Use permissions give rights to 'use, display and include' this listing.
Distribute	Distribute permissions allow users to 'use, display and include' the listing in other published listings in the sharing economy, created by the downloader account.
Modify/Remix	Modify permissions allows rights to make derivatives, modifications, and alterations on this listing and furthermore 'use, display and include' this altered version in other listings published in the sharing economy. The original Creator's account must be credited on the listing page.

Final Process for Determining Users' Ability to Interact with Content

The process to determine a user's permission to access, share, re-use, and modify content based on content's attributes (determined by Data Rights or Creative Commons, Distribution Statements, and Limited Dissemination Controls) is also dependent on the user's attributes and role. However, the contents attributes are the key to the process. Additionally, it was determined that non-government users should be given the option to use Creative Commons options instead of the negotiated data rights associated with the content since these permissions are commonly used in the commercial sector. However, users should not have the capability to restrict permissions to a degree greater than those data rights already stated. In other words, users can make their content more accessible, but not less than the existing data rights. Content created and added to the ecosystem by members of the DoD do not have the opportunity to apply Creative Commons and must adhere to the guidance associated with the applicable Distribution Statements.

In a similar vein, it was determined that non-government users should be able to increase their permissions in a robust fashion to encourage and increase collaboration. Therefore, it was determined that these users could adjust permissions to give increased access to individuals, groups, teams, and other companies within the sharing economy. For example, a vendor may create a new listing within the sharing economy that was developed under SBIR data rights, but they want to share that listing with a particular partner vendor so that the partner can use the listing within their own application. In this instance, the original vendor would indicate SBIR data rights (which enables ONLY Government users to Discover, Download, Use, and Distribute), but then also indicate that the partner vendor can *Use* the listing as well. In the permission matrix, the partner vendor would be able to Discover, Download, and Use the listing from within the sharing economy Hub.

Permission Framework Summary

To enable a sharing economy that encourages participation and fosters collaboration, the following considerations were implemented into a robust permission framework:

- User Type – To protect IP and sensitive government data, a permissions framework must have a deep understanding of the user type and role (e.g., DoD Personnel, DoD Contractor, Foreign National, etc.
- Data Rights – To ensure contractual obligations are met, a permissions framework must account for contractual and negotiated data rights
- Classification of Government Data – To protect government data, the permissions framework must establish the classification of government technical data (e.g., Is the data unclassified, controlled unclassified information (CUI), or classified?)
- DoD Distribution Statements and Limited Dissemination Controls – To further protect government data, DoD distribution statements and LDCs must be taken into account within a permissions framework, especially as it related to user type (e.g., per DoD regulations, who can access the technical data?)
- Creative Common Licenses – To protect vendor IP, a permissions framework must allow creative commons license types
- Permissible Content Interaction Types – A permission framework must further delineate what exact functions users can do with the data/content that is listed within the sharing economy

- Releasability – An approval for public release with unlimited distribution (USA, default) and foreign governments (with approvals)

This matrix of combinations was built into the centralized Hub and platform interface that was networked via a managed user network that controls centralized user permissions and roles. Combined, the permissions framework and identity and access managed network ensures that proper permissions are granted and persistently enabled. However, to be useable, accessible, and properly implemented, a user-facing tool must exist so that users can correctly assign appropriate permissions to their hub listings within a sharing economy. Towards this end, a Permission Wizard tool was developed and implemented to provide a front-end application in which sharing economy contributors could assert their permissions with the centralized Hub. A Permission Wizard tool was implemented to walk users through different permission options in a linear fashion based on their answers to set questions. At the end of the questions, a permission setting was displayed, and users could further adjust permissions to be more open (e.g., allow more user types of various levels of access) as desired. The permission wizard tool was created to be run on the Hub but also to be an API call from decentralized platforms that would allow a contributor to use the Wizard inside of third-party applications.

Instantiating 'Permission Wizard' into Hub

As previously mentioned, a step-by-step linear permission wizard tool was developed and instantiated within the sharing economy to streamline and easily enable the settings of content permissions. As a government participant in the sharing economy providing access to government technical data, a user would first launch the permission wizard tool, provide the classification level, indicate the distribution statement or LDC marking associated with the classification level, review the suggested permissions and settings, and finally approve and apply the permission settings. As a third-party vendor participant in the sharing economy providing community access to their content, a user would first launch the permission wizard tool and then indicate if the content was developed under a government contract. If the content was not developed under a government contract, then the user would proceed to apply which creative commons license applies to the content. If the content was developed under a government contract, the user would then be promoted to indicate which type of government contract the content was developed for. If the user selects "SBIR", then SBIR data rights are applied. If the user selects "OTHER," then they are given the opportunity to indicate which data rights apply to their content. Once data rights or creative commons are asserted, if the asset is non-CUI, the user is then able to review the suggested permissions, modify by increasing access level as desired, and then approve and apply the final permission settings. In the case of CUI data, a LDC can then be set (Figure 1) that further controls dissemination permissions available. Once permissions are accepted and asserted, the listing is available within the platform interface of the centralized Hub for the sharing economy where other users can discover, download, use, distribute, and modify the listing as appropriate for their user type and the asset's asserted permissions. It is important to note that only the content contributor or contributor organization associated with that asset listing can set, modify, and control their content listing permission settings.

PILOT PROGRAMS TO EVALUATE PERMISSIONS FRAMEWORK

The preliminary implementation of the central Hub collaboration framework to support the sharing economy has shown some promising initial results. Initial feedback was received from three separate pilot programs conducted with USAF units and USAF contracted third-party vendors.

In the first pilot program, instructors from the 367 TRSS ("The Griffin") participated in the evaluation. The 367 TRSS is a training squadron that develops and deploys Air Force Specialty Code (AFSC) maintenance related training for use across the entire Air Force. In this pilot program, they uploaded official training content onto the centralized Hub network for other USAF training units to make use of. TSgt Erik Jacobson indicated "*The current version of the Permission Wizard has been extremely helpful and fast to use. As a content creator who deals with creating CUI training, classifying the training appropriately is a requirement for us. This tool has made it very easy to do with its pre-load settings and simple to navigate interface.*"

In the second pilot program, 15 USAF-contracted industry vendors uploaded content onto the centralized Hub for the sharing economy. These vendors spanned multiple XR training categories, including XR Low-Code Development Tools, AR/VR Training, Self-Authoring Tools, Peripherals (e.g., Haptic gloves, Motion Simulators), and more. One of the biggest trepidations of companies contributing content was other companies violating their intellectual property rights or data rights. Once it was shared how the permission wizard framework would allow them to control their content IP, they all felt comfortable to share their content into the Hub. To date, over 50 pieces of "content" have been listed through the sharing economy. There have been no reported instances of permissions being violated, indicating that IP has been protected from other potential competitors within the sharing economy.

In the third pilot program, the AETC Maintenance Training Next program utilized the sharing economy to develop a new version of their Crew Chief Fundamentals Course, which included technologies such as AR, VR, and AI. The USAF Crew Chief (AFSC 2A3X3) Fundamentals Course was completely developed using nine different types of media, including technology from four different third-party vendors (2 VR training platforms, 1 mobile AR training platform, and 1 AI engine), comprising over 170 lessons in 4 levels – all developed using content that was provided within the sharing economy. In this pilot program, USAF users were able to discover and use third-party vendor content that was provided through the sharing economy – even though that content may not have been developed specifically for that particular USAF unit. This demonstrated the ability for the USAF to re-use content it already paid for under other government contracts and for third-party vendors to become connected to new USAF units. In this pilot program, there were no reports of permissions being violated.

FUTURE RESEARCH AND CONSIDERATIONS

The work this paper describes focuses on the "sharing" part of the sharing economy. All the participants, vendors, and applications had contracts with the USAF that established the data rights of the digital assets tracked and stored in the Hub. Ensuring that a central Hub respects data rights, incentivizes contributors and fuels a collaborative ecosystem is imperative to its success. Future work should look at the other considerations presented in this paper, including programmatic considerations such as consolidating other consortiums of technologies into a centralized sharing economy and determining which government entities are responsible for ownership and maintenance of such a robust sharing economy.

The sharing economy presented herein enabled competition while avoiding divergence through sharing via the robust permission wizard tool that protects IP and data rights. Future work is needed to determine additional incentives for participating in the sharing economy. In this vein, there are several contracting considerations that must be worked through to ensure the success of the sharing economy. While in the current instantiation, vendors were not provided the prospect to engage with additional contracting/purchasing opportunities. The sharing economy must ensure that ecosystem vendors can secure additional funding through participation; perhaps there is even an opportunity to enable direct purchasing within the sharing economy to fuel innovation with contracting and acquisitions.

Finally, the current instantiation of the sharing economy focused on innovative, net-gen technologies. However, legacy systems are crucial for military training success. Future research will need to determine and architect the best approach for developing and implementing open APIs that provide backwards compatibility for updating older assets and ensuring they still work with legacy systems.

CONCLUSION

The U.S. Government requires that training systems of the future be built leveraging MOSA and be composed of integrated technologies that are easily accessed, updated, and shared. To realize this requirement, the current paper posited that a sharing economy was necessary to enable collaborative consumption across the DoD and industry. Importantly, the sharing economy must consider how permissions are implemented across the ecosystem of technologies to protect vendor IP, data rights, and sensitive government data.

One of the biggest concerns in the development of this initial sharing economy was that companies would not be willing to participate in it. The current implementation requires companies to integrate their digital asset listing to a MOSA platform via APIs, and ideally make their assets available as widely as possible, even if not contractually obligated. There are multiple ways companies can share their content; they can either host their content on the hub or simply provide the link to their content via APIs wherein tagging and permissions still take place. However, it has been found that many companies are generally willing to do so. This implementation of the sharing economy provides them with advantages. They can focus on spending time and energy on the aspects of the training ecosystem that they know best. By integrating with the MOSA platform, they do not have to develop back-end features like authentication, user permissions, and Learning Management System (LMS) integration, instead leveraging those APIs. They also get a wider network for discovery and distribution with no additional work on their part. Thus, it was found that third-party vendors had several incentives to share their content within the sharing economy – especially smaller businesses who found immense value in being connected to new USAF units, end users, and stakeholders.

The present paper presented a framework for an open sharing economy in which government and third-party vendors could distribute and discover content associated with their current works. Several companies and USAF units participated in pilot programs that demonstrated the utility of such a sharing economy and vetted a novel permissions framework that protected IP, data rights, and government security of technical data. The permission framework presented in the present paper provides a mechanism for ensuring safe participation within a sharing economy. Future work should determine the return on investment of the proposed approach and provide a cost-benefit analysis. Additionally, more work is needed to determine the optimal approach for incentivizing and motivating third-party vendors and government organizations to participate in the sharing economy.

REFERENCES

Bonciu, F., & Balgar, A. C. (2016). Sharing economy as a contributor to sustainable growth, an EU perspective. *Romanian J. Eur. Aff., 16*, 36.

Champney, R. K., Stanney, K. M., Milham, L., Carroll, M. B., & Cohn, J. V. (2017). An examination of virtual environment training fidelity on training effectiveness. *International Journal of Learning Technology, 12(1)*, 42-65.

Creative Commons Corporation. (2020). *About CC Licenses*. Creative Commons.

Creative Commons Corporation. (2021). *About The Licenses*. Creative Commons.

Creative Commons Corporation. (2022). Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Curtis, S. K., & Lehner, M. (2019). Defining the sharing economy for sustainability. Sustainability, 11(3), 567.

Defense Information Systems Agency. (2021). *Data Rights*. DISA.

DFARS 252.227-7017

DoDI 52230.24 Distribution Statements on Technical Documents, August 23, 2012, Incorporating Change 3 Creative Commons

Heinrichs, H. (2013). Sharing economy: a potential new pathway to sustainability. *GAIA-Ecological Perspectives for Science and Society, 22*(4), 228-231.

Heo, Y. (2016). Sharing economy and prospects in tourism research. *Annals of tourism Research, 58*, 166-170.

Hossain, M. (2020). Sharing economy: A comprehensive literature review. International Journal of Hospitality Management, 87, 102470.

Poentizsch, J. (2018). What's the difference between Decentralized and Distributed? *nakamo.to.*

VMWare (2022). Federated Network.

Kelly, M. D. (2019). *AF Instruction 17 - 701*. Air Force Instruction 10-701.

Koetsier, J. (2015). The Sharing Economy has created 17 billion-dollar companies (and 10 unicorns). *Venture Beat.*

Puschmann, T., & Alt, R. (2016). Sharing economy. *Business & Information Systems Engineering, 58*(1), 93-99.

Richardson, L. (2015). Performing the sharing economy. *Geoforum, 67*, 121-129.

SP 800-207, Zero Trust Architecture

10 USC 4401: Requirement for modular open system approach in major defense acquisition programs; definitions

Watry, K. E., Pardon, C. K., & Merkle, M, T. (2021). Lessons from the Front Lines: A Modular Open Systems Approach to a Training Ecosystem. In *Proceedings of the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) Annual Meeting*, Orlando, FL.

Wosskow, D. (2014). *Unlocking the sharing economy: An independent review* (p. 43). London, UK: Department for Business, Innovation and Skills.