Dynamic Mobility Applications Open Source Application Development Portal

Task 4: System Requirements Specifications

www.its.dot.gov/index.htm

Final Report – October 12, 2016

FHWA-JPO-17-490

U.S. Department of Transportation

Produced under DTFH61-06-D-00005
Task Order: Dynamic Mobility Applications Open Source Application Development Portal

ITS Joint Program Office
Research and Innovative Technology Administration
U.S. Department of Transportation

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

1. Report No.
FHWA-JPO-17-490

2. Government Accession No.

3. Recipient’s Catalog No.

4. Title and Subtitle
Dynamic Mobility Applications Open Source Application Development Portal – System Requirements Specification

5. Report Date
October 12, 2016

6. Performing Organization Code

7. Authors
Steven Le, Diane Newton, Ron Schaefer

8. Performing Organization Report No.

9. Performing Organization Name and Address
Leidos
11251 Roger Bacon Drive
Reston, VA 20190

10. Work Unit No. (TRAIS)

11. Contract or Grant No.

12. Sponsoring Agency Name and Address
United States Department of Transportation
Intelligent Transportation Systems Joint Program Office
1200 New Jersey Ave, SW
Washington, DC 20590

13. Type of Report and Period Covered
August 2010 – October 2016

14. Sponsoring Agency Code
ITS JPO

15. Supplementary Notes
Randy Butler, COTM

16. Abstract
This document describes the System Requirements Specifications (SyRS) of the Dynamic Mobility Applications (DMA) Open Source Application Development Portal (OSADP) system in details according to IEEE-Std. 1233-1998. The requirement statements discussed here was used as the one of the key references for the system design and construction process.

17. Key Words
Open Source, Application Development, Cloud Hosting, Dynamic Mobility Applications

18. Distribution Statement
No restrictions.

19. Security Classif. (of this report)
Unclassified

20. Security Classif. (of this page)
Unclassified

21. No of Pages
80

22. Price
N/A

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

No table of figures entries found.

Chapter 1. Introduction

1.1 System Purpose

This document describes the System Requirements Specifications (SyRS) of the Dynamic Mobility Applications (DMA) Open Source Application Development Portal (OSADP) system in details according to IEEE-Std. 1233-1998. The requirement statements discussed here was used as the one of the key references for the system design and construction process.

1.2 System Scope

The building of the DMA OSADP system is a USDOT sponsored initiative to promote open source development. Initially the system will be used for developing several USDOT DMA program application bundles, as shown in Figure 1. However, the system architecture also allows new projects to commence from within the user community. Mobility applications developed will share data needs with safety and environment applications of the Intelligent Transportation Systems (ITS) program.

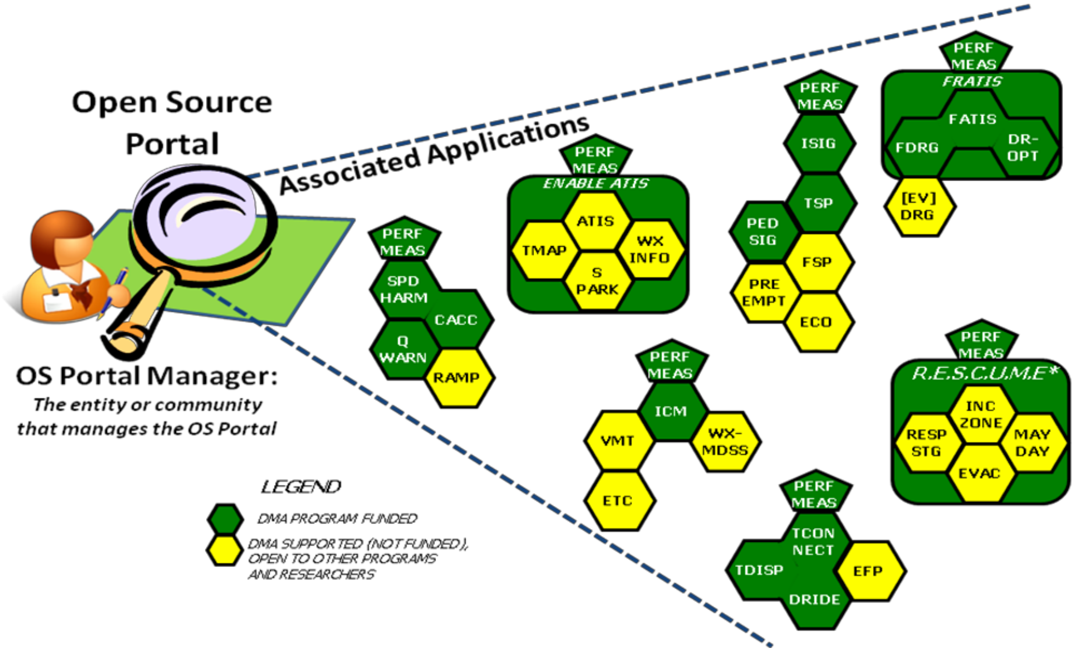

Figure 1-1. USDOT DMA Program Application Bundles

Source: Joint Program Office Intelligent Transportation Systems Website

The OSADP system will realize the capabilities discussed in the Concept of Operations, which was built from cumulative knowledge and understanding gaining from the User Needs workshops and the Assessment of Open Source Development Web Resources exercise. This system will not be all-encompassing but rather scope specific, focusing on USDOT mobility application development in open source approach.

At a high level, the DMA OSADP is essentially a web portal that cultivates and promotes a friendly and collaborative community that develops transportation mobility applications.

1.3 System Overview

The Dynamic Mobility Applications (DMA) Open Source Application Development Portal (OSADP) system is an integration of three main subsystems, powered functionally by enabling technologies and applications. The system operates on a scalable computing infrastructure for providing a secured yet open environment for facilitating maximum collaboration among the users. It consists of the following:

- **Subsystems**, providing the primary functionality for the three tiered architecture environments
- **Enabling technologies and applications**, providing supportive computing services, communicating and software development based applications to the environments
- **Computing infrastructure**, providing hardware and software resources necessary for a robust environment which may need to scale up resources on demand.

Together the above computing subsystems and components were integrated to become the DMA OSADP system.

The main subsystems powered by the enabling technologies, applications, and services provide the foundation for the system. Boundaries of the subsystems are not to be defined in terms of discrete and independent systems, but by access privileges associated with the user roles.

As described in the Concepts of Operation document and shown in Figure 2, the DMA OSADP is a tiered architecture system. Activity in each tier is regulated by terms and conditions agreed to by the users during the registration process, prior to granting user access. Every registered user also accepts the terms of the governance and portal policies.

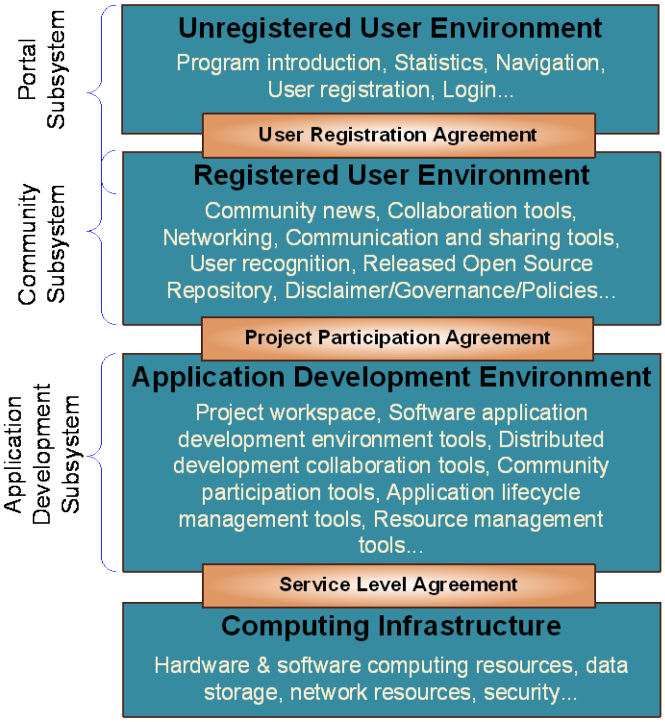
Portal Subsystem
Community Subsystem
Application Development Subsystem
Unregistered User Environment
Program introduction, Statistics, Navigation, User registration, Login...
User Registration Agreement
Registered User Environment
Community news, Collaboration tools, Networking, Communication and sharing tools, User recognition, Released Open Source Repository, Disclaimer/Governance/Policies...
Project Participation Agreement
Application Development Environment
Project workspace, Software application development environment tools, Distributed development collaboration tools, Community participation tools, Application lifecycle management tools, Resource management tools...
Service Level Agreement
Computing Infrastructure
Hardware & software computing resources, data storage, network resources, security...

Figure 1-2. DMA OSADP's 4-Tier Architecture

For most users, access to portal resources is pre- determined by user roles. User access to system resources is based on permissions which may have access privileges grouped into access types based on the functional role of the user. For instance, a visitor may only have limited access to system resources and may see only public news and information. A registered user, on the other hand, may access to community resources such as the discussion forums and released source code repository after completing the user registration and agreeing to the system terms and conditions. By agreeing with additional terms regarding project participation, project contributors have access to all that a registered user has, plus the ability to access to project workspace and other resources in the application development environment.

A Service Level Agreement (SLA) will be signed with hosting and service providers committing to providing a high level of service quality of computing infrastructure, resources and technical support services for the system.

In brief, the DMA OSADP system is an integration of existing subsystems with enabling technologies and applications that build a cohesive user community sharing interests in developing open source transportation mobility applications.

Chapter 2. General System Description

2.1 System Context

The DMA OSADP system, as shown in Figure 2-1 above, directly correlates to the three primary tiers of the system architecture. Multiple applications and enabling technologies are integrated into and upon these subsystems to provide the required system functionalities.

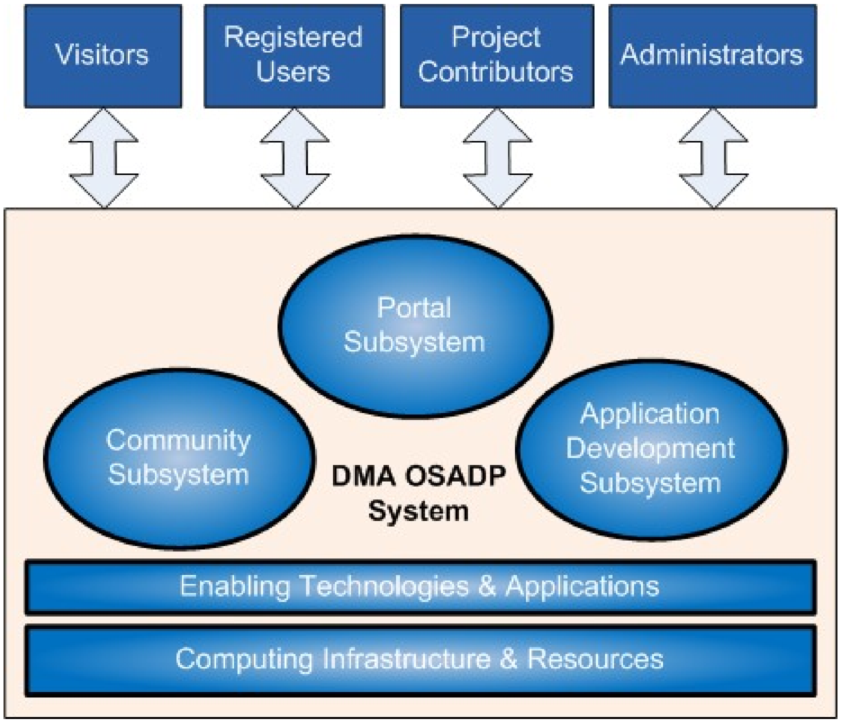

Figure 2-1. DMA OSADP Functional System Components Overview

To achieve cost effectiveness, data security, infrastructure scalability, and other benefits, the DMA OSADP system is hosted at a cloud computing location where computing resources and computing infrastructure are provisioned automatically and customized for meeting the system needs. The system requirements can be built up from Platform as a Service (PaaS) or Software as a Service (SaaS) which come with enabling technologies, applications and services to be customized and configured. A number of available cloud hosting SaaS solutions come with basic portal, community, and application development functionality provided. If a SaaS solution is selected, extensive customization and configuration may be required to provide the specific look-and-feel for the USDOT DMA environments.

The following sections describe key features of the subsystems and related components. For each portal environment, user class profiles and associated roles are explained in details in Appendix C.

2.1.1 Portal Subsystem

The Portal Subsystem (PS), as shown in Figure 4, consists of services that work collectively for rendering the portal environment including the web server, content management system (CMS) application, and user registration and management. It operates the environment interfacing with the public and registered users. Visitors come to DMA OSADP via the web entry of the Portal Subsystem known as the web portal, while other users may come through other authenticated entry points. For instance, a developer may access the application development environment via the integrated development environment (IDE) application software or the system administrator may enter through a back-end access path which is hidden from regular users.

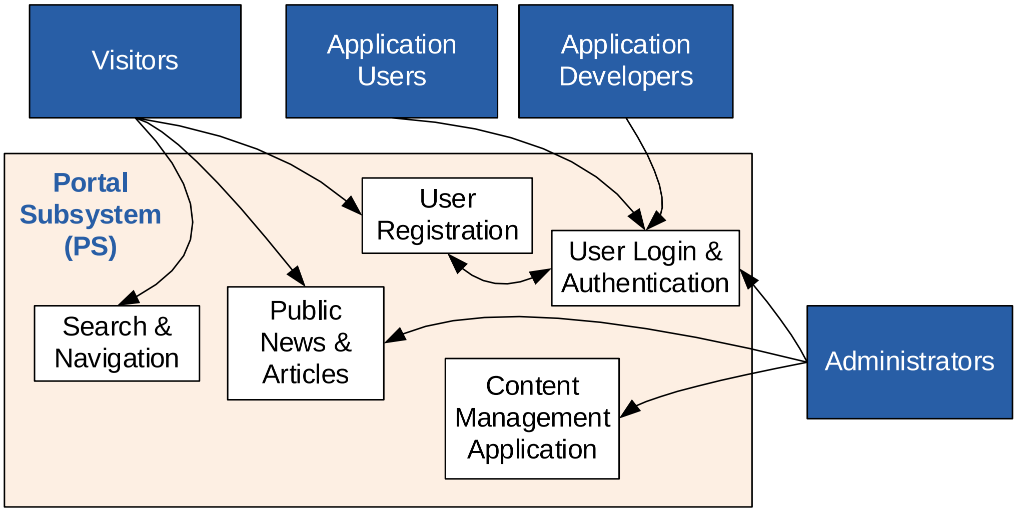

Figure 4 - Portal Subsystem's Functional View

The Web portal makes available to the Internet users news and information about the DMA open source development program and is shown visibly on the website. Content of the portal includes materials updating the DMA changes and other information of interest to visitors encouraging them to join and collaborate with others on the DMA community.

Interested visitors can become a member of the DMA community by completing the user registration. By following the “User Registration” link shown conspicuously visitors can complete the User Registration form. Similarly, to communicate with the person in charge of the portal, visitors can click on the “Contact Us” link shown visibly on the public portal to compose a message to be routed to Portal Manager.

2.1.2 Community Subsystem

The Community Subsystem (CS), as shown in Figure 2-2, operates a collaborative content and knowledge management site for USDOT and affiliated users to connect and share information. Among the many communication tools and channels for supporting the community are the user collaboration tools such as group discussion forums, user blogs, networking application, etc.

Accessible by all registered users who agreed to terms and conditions of the community during the registration process, the community operates per the site governance and operational policies.

The DMA OSADP community promotes active collaboration among the registered users. It allows project team members and individual user to connect, explore, discuss, collaborate, and share useful information with one another.

It is not required for an individual user to be working on a development project to impart knowledge and experience while contribute and share with the community. For interaction with those who develop the applications, certain discussion forum threads and topics are dedicated as channels for registered users and project contributors to exchange information and cooperate with each other. User groups can be built around a community of interest based on mission areas, technologies or specific project types.

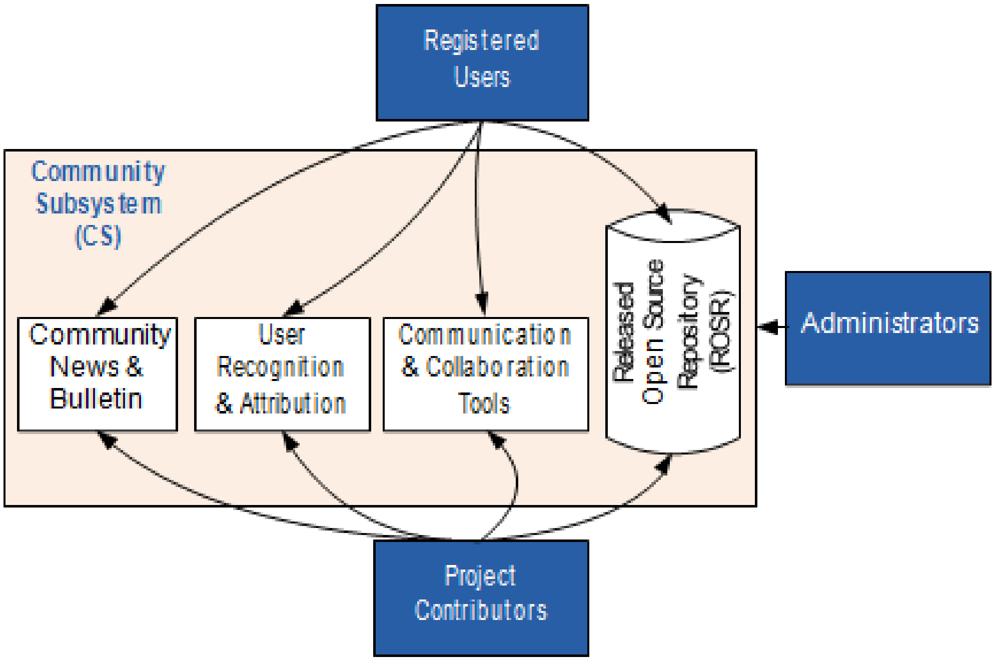
Registered Users
Community Subsystem (CS)
Community News & Bulletin
User Recognition & Attribution
Communication & Collaboration Tools
Released Open Source Repository (ROSR)
Administrators
Project Contributors

Figure 2-2. Community Subsystem's Functional View

The community's diverse talent pool offers great potential for generating new ideas and solving problems that otherwise may not be possible with a traditional single purpose project team.

In addition to a common library that was implemented for storing community documents, one of the key features of the CS is the hosting of the Released Open Source Repository (ROSR). Source code developed in the Application Development Environment can be uploaded to the repository for the all community members to access.

The CS features a set of tools and services that aim to promote a cohesive community around transportation application development interests.

2.1.3 Application Development Subsystem

While the Community Subsystem has a broad and nonspecific scope, the project teams working in the DMA Application Development Subsystem (ADS) had a project- specific focus for realizing and implementing individual project operational concepts.

The ADS, as shown in Figure 6, enables a collaborative software development for distributed members by providing a range of communication and collaboration tools that allow the project members to share ideas, convey thoughts, and work together effectively. The environment features a suite of development applications tools such as software version control, bug and issue trackers, and release management tools. Software compilers for various programming languages are linked and integrated with the environment as required. For project management, the ADS offer application lifecycle management including project schedule, system development methodology, requirement management matrix, and milestone tracker, etc. For the project team, shared workspace and resources are instantiated upon project commencement and additional resources can be provisioned dynamically. Online documentation tools such as wiki and project webpage are offered for promoting maximum collaboration among geographically distributed developers.

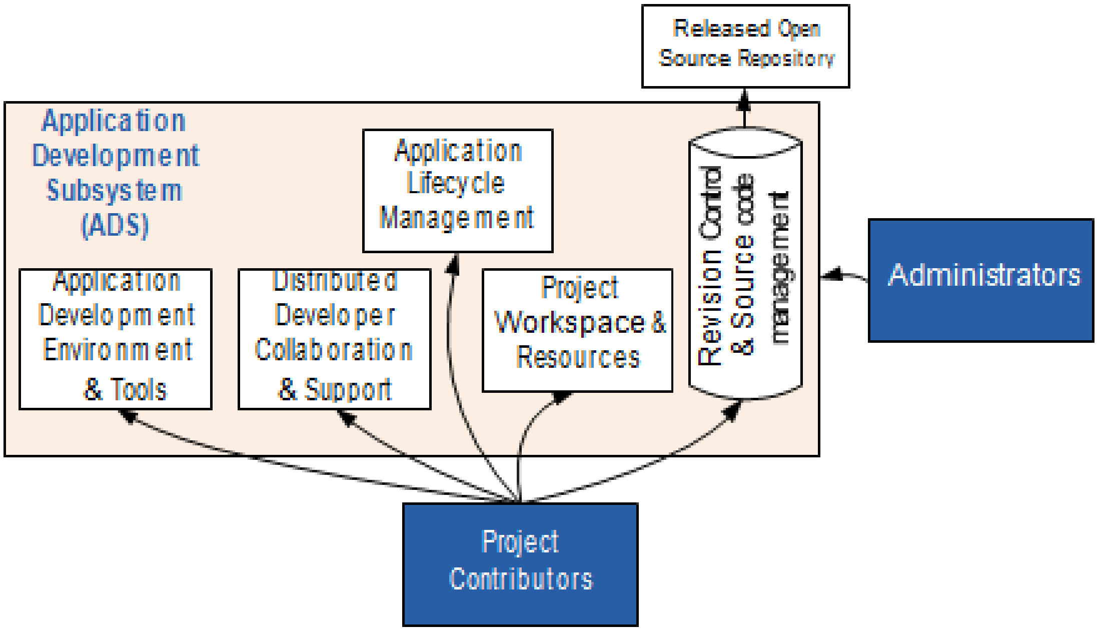
Released Open Source Repository
Application Development Subsystem (ADS)
Application Lifecycle Management
Revision Control & Source code management
Administrators
Application Development Environment & Tools
Distributed Developer Collaboration & Support
Project Workspace & Resources
Project Contributors

Figure 2-3. Application Development Subsystem's Functional View

In-development application source code is kept in a revision control and source code management system. As the main repository for all dynamic mobility application code base, these files and folders are well maintained and backed up frequently. Applications that have undergone quality control and are deemed stable may be uploaded to the ROSR and made accessible by the community.

2.1.4 Enabling Technologies

Following are a select few of many enabling technologies and solutions that can be integrated with the system to empower its users.

User Security and Resource Management

As a part of the computing infrastructure layer, a system security module enforces compliance with data security standards to protect the portal and its environments. The security standard includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures, intended to proactively protect data and other intellectual assets. Using cascading role-based access controls, permission is set for distributed workgroups by project, sub-directory or IP address which makes it easy to control who can do what and where.

To protect the operational environment from potentially harmful malware and planted viruses, a security service will scan frequently for virus infection and detect any malware on the system. This security scan and sweep operation is done regularly to ensure the environment is clean and safe for sharing documents and source code.

The system security module also supports the Portal Subsystem in monitoring the user to prevent against abuse or hacking of the registration process.

System administrative users are equipped with resource management tools for making allocation and procedures for processing and approving various requests. It allows specific administrative users to manage users, projects and associated resources. This application can add users and quickly sets up permissions, email lists and notifications, including a procedure to instantiate a new project and allocates associated resources, workspaces for multiple project members based on qualified request. Permission assignment and access control for all users are managed by this technology.

Content Management (CM)

Webpage, articles, portal content, etc. may change frequently. A content management application was implemented to establish structured procedures for managing content updates and addition. The content management is role-based access controlled, allowing certain users to perform review and approve changes on a workflow process.

2.1.5 Applications, Tools, and Services

Collaboration Tools

The collaboration application consists of a number of tools and services including discussion forum, social networking utility, instant communication with peers, etc. The purpose of these applications is to enable users to communicate and to promote maximum cross pollination of ideas between community members. Both the DMA community members and project contributors can use these tools in their respective environments. Appendix C describes the roles of the Portal Manager and Portal Moderators in managing and promoting collaboration tools. Accessing to these communication tools are managed based on user privilege and access rights.

Release Management

The release management application is an integration of a number of existing applications performing source control, document management and revision management. This application allows project team members to manage the constantly changing application development cycles. Source code repository keeps the software changes in revision branches and allows certain project members to request software builds and releases them to the ROSR based on maturity and stability of the code.

Application Lifecycle Management

The project management application is an integrated suite of web-based tools for managing application development lifecycles. The Project Manager and members can view project details and track the project progress more cohesively.

Centralizing management of users, projects, processes, and IP assets online improves project visibility and increases productivity. The application supports several software development lifecycle management methodologies including Agile, waterfall, or a hybrid approach.

2.2 System Modes and States

This section outlines the different modes of operation of the OSADP system. By design, the system is modular and in some cases, each module can operate independently. For instance, the public website Portal can be segregated and taken down for maintenance without affecting the Application Development Environment. The configuration management application in the Application Development Environment can also be independently disabled temporarily to be serviced while others remain operational. The system operates in the following modes:

Operational Mode - In normal condition, the system is fully operational non-stop around the clock and year round. While running in this mode, the system provides portal services and users can access the portal content at each tier. The general public can visit and view content on the Public Portal; Registered Users can access community features and capabilities in the Registered User Environment; and Project Contributors can collaborate and develop applications simultaneously.

Restore Mode - This mode is used when the system must be restored from a backup that has been completed in a previous time period as a result of a malicious attack or an internal error that brings down a portion of or the entire system. While in this mode, some portal services may be unavailable to the users until data restoration is completed. At that time, the system can be switched back to Operational Mode. In isolated incidents, the restore operations may be performed to recover only a corrupted section without affecting the rest of the system.

Upgrade Mode - As needed, this mode can be active when the system goes through a maintenance upgrade to bring the system functionality up-to-date with the latest revision. During this mode, users may have limited access to the portal contents, although the downtime is typically brief. This mode should be scheduled in advance, with notices sent to members and posted to community bulletins clearly announcing when this upgrade operation will be performed and when it’s expected to recover fully. Upon completion, the system will switch back to Operational Mode.

2.3 Major System Capabilities

At a high level, the DMA OSADP system offers the following major capabilities:

Public Portal - Open to the public, a general portal is accessible to everyone on the World Wide Web, where general information is made available. Visitors are able to see:

- News and information about the system environments
- Descriptions of DMA on-going projects
- User registration information on how to become a registered user and gain access to the Community resources in the Registered User Environment

Registered User Environment - By completing the user registration and following approval after an evaluation process, an unregistered user may become a registered user and gain access to community resources and communication tools available at this level including:

- Collaboration tools
    - o Discovering and joining user groups

    - Sharing ideas and exploring other ideas
    - Participating in discussion forums
    - Sharing knowledge, experience and lessons learned
    - Forming new product ideas and proposing new projects
    - Finding answer and solutions
    - Social networking communicating with other community members
    - Recognizing and giving attribution to community contributors
- Released Open Source Repository
    - Ability to download DMA application source code and associated core assets
    - Sharing application source code and enhanced source code derived from the base application code from this site
    - Contributing non-source code core assets such as test data, algorithms, etc.
    - Reporting application bug and issues

Application Development Environment - This environment is accessible mainly by project contributors, a class of registered users who directly participate in the development of the application. Access to this environment is granted either through a USDOT project bid-and-proposal award or an approved community-initiated project idea. Before becoming a member of this collaborative development environment, users are required to accept additional terms and conditions specified in the project participation agreement, which stipulates a range of operating policies including IP and responsibility to the development team and its objectives.

The main capabilities of this environment include:

- Software development tools and resources:
    - Code management
    - Software configuration management
    - Application lifecycle management
    - Project webpage
    - Project team workspace
    - Project hosting
    - Developer resources
    - Online documentation
    - Issue management and bug tracking
- Collaboration tools for distributed development team members

Stable application source code developed here may eventually be available in the ROSR in the Registered User Environment.

A Contributor of one project may be able to participate in another, depending on interest, skills, affiliation, and status of funding; this involvement will be evaluated case by case basis by the Project Manager and Project Sponsor.

Computing Infrastructure – The system is hosted at a commercial hosting facility that allows distributed users to reach the system resources from any network locations. The computing infrastructure has at minimum the following:

- Ability to scale up computing resources to meet demand, including: adding CPU, memory, data storage, network bandwidth, etc. within short turn-around time.
- System environments follow best practices for data security according to the
- PCI Security Standards Council, securing data at-rest as well as in-transition.

2.4 Major System Conditions

1) Registered users and visitors are able to view the public portal website via one of the major Internet browsers, which follows the formal standards and other technical specifications that define and describe aspects of the World Wide Web.
2) The system operates non-stop around the clock and year round, and is accessible from a network environment.
3) Registered users are able to access the DMA community environment to collaborate with other community members.
4) Application Development Subsystem users are able to access authorized project team workspace and resources.
5) System administrator(s) are able to access all system environments, including configuration panels of all subsystems.

2.5 Major System Constraints

The IEEE 1362 standard defines operational constraints as limitations placed on the operations of the proposed system. OSADP system constraints include:

1) The system supports multiple development applications that runs on system platforms such as Windows, Linux, etc.
2) The system supports multiple programming languages. The Application Development Environment does not restrict to a particular type of programming language.
3) The system is scalable to support the development of specific USDOT Dynamic Mobility Applications and other future applications that have not been identified.
4) The system supports commercial-off-the-shelf (COTS) computing equipment and software.
5) The Portal Subsystem complies with Section 508 of the Rehabilitation Act and the Access Board Standards.
6) The system manages open source applications according to open source licensing agreement chosen for the released application.
7) The system manages open source applications according to the Governance defined by USDOT.
8) The system fully complies with federal policies, regulations, and guidelines regarding restrictions on the foreign export of federally-funded research materials.

2.6 User Characteristics

Generally, users of the system are classified into five user class categories:

Unregistered User - Any user who has access to the Internet can visit the OSADP. Content access is limited for Unregistered Users.

Registered User - An Unregistered User who completes the online registration form and agrees to terms of user agreement is evaluated whether they can become a Registered User. Once approved, a Registered User can view additional content, participate in discussion, and is able to download any content made available in the ROSR.

Contributor - A number of user classes are defined in the Contributor category; users in this category participate directly in projects. Each user may be identified with a single or multiple projects in various roles. Users of this category sign and accept additional terms and conditions in the project participation agreement which may include stipulation on IP, governance policies, and open source license terms. A Contributor may assume various project responsibilities such as Project Manager, Developer, Committer, Reviewer, Tester, Technical Writer, etc. A Contributor may participate in multiple projects and assume different roles. Other roles may be created as necessary.

Administrator - Several user classes are grouped into the administrator category. Generally, these users provide oversight and stewardship functions of one or multiple OSADP projects, and they are not restricted to any particular tier. Project Sponsor, Portal Manager, Governance Administrator, and System Administrator belong to this category. Depending on their specific role, an Administrator may or may not have read or write access to the project files and documents in the Application Development Environment.

Infrastructure Provider - Not participating in project activity directly, this type of user provides the computing infrastructure services to the OSADP environment. The Infrastructure Provider interfaces with the OSADP System Administrator to ensure infrastructure resources are allocated as expected, and computing environments are functional at optimal capacities.

The Infrastructure Provider role is not discussed as a user category since this resource does not participate in the core activities of OSADP.

Appendix C shows a summary of the user categories and classes with role descriptions, details on permissions, access privileges, and capabilities.

2.7 Assumptions and Dependencies

2.7.1 Governance

2.7.1.1 Detailed governance were written by USDOT and made visible as appropriate to registered users on the portal.

2.7.1.2 Registered users agree to terms and conditions for completing the user registration.

2.7.1.3 Procedures and processes were created for managing the routines.

2.7.2 Content

2.7.2.1 Initial open source content including source code and core assets were loaded into the system's ROSR.

2.7.2.2 Applications developed from projects were slowly populated into the ROSR.

2.7.3 Operations

2.7.3.1 The system is operated by Leidos, a contractor working on behalf of USDOT.

2.7.3.2 The system is hosted in a commercial hosting facility that meets USDOT IT and security standards.

2.8 Operational Scenarios

In the Concept of Operations document, 35 operational scenarios were discussed. They are referenced in Appendix B and referred to by the requirement matrix later in this document.

Chapter 3. System Capabilities, Conditions, and Constraints

3.1 Physical

These requirements describe the system construction and integration, including the environmental conditions.

3.1.1 Construction

3.1.1.1 The system integrates and utilizes existing components from COTS products and open source technologies. A new system component would have been built only if it did not already exist.

3.1.2 Durability

3.1.2.1 The system software and hardware selected provides an upgrade path so future enhancements can be made to reflect future requirements.

3.1.3 Adaptability

3.1.3.1 Core assets and application source code are kept in a configuration management system that complies with industry standards to ensure portability.

3.1.3.2 System resources such as CPU, memory, data storage, network bandwidth, etc. can be increased or decreased within 5 working days of the request.

3.1.3.3 The system allows the graphic user interface (GUI) to be configured and customized by the System Administrator.

3.1.3.4 The system provides the capability for authorized development team members to edit the project webpage.

3.1.4 Environmental Conditions

3.1.4.1 The hosting provider for DMA OSADP system meets USDOT's IT standards and guidelines.

3.1.4.2 The primary language of the DMA OSADP website is English.

3.1.4.3 Besides scheduled maintenance events, the system operates non- stop around the clock and year round.

3.2 Performance Requirements

These requirements describe how the system performs.

3.2.1.1 The Community Subsystem provides the capability to support over 300 users.

3.2.1.2 The Community Subsystem provides the capability to host a minimum of 40 concurrent applications and associated documents in the ROSR, with the ability to scale up storage capacity to accommodate additional applications.

3.2.1.3 The Application Development Subsystem provides scalable computing resources including CPU, memory, network access and bandwidth, data storage capacity, etc. within 5 working days after the request is formally submitted.

3.3 Security Requirements

The following requirements protects the system data at rest as well as in transition, from malicious hackers and bad users.

3.3.1 Security Subsystem

3.3.1.1 The Security Subsystem provides the capability to immediately detect, eliminate or quarantine viruses from infected uploaded items before storing them into the ROSR (UN5.3).

3.3.1.2 The system is upgraded to include all critical security patches within 5 business days after they are available.

3.3.1.3 The Security Subsystem provides the capability for Portal Manager to review and approve all content added to the ROSR (UN8.5).

3.3.1.4 The Security Subsystem provides the System Administrator the capability to see login history for users of the portal (UN8.8).

3.3.1.5 The Security Subsystem provides the capability to prevent unauthorized access into computers and computer networks via all access points with strong security validation and authentication (UN8.3).

3.3.1.6 The Security Subsystem provides the capability to comply with PCI Security Standard Council recommendations and security best practices.

3.3.1.7 The Security Subsystem provides the capability to display an audit trail of modified files and history of major changes to application source code and files (UN8.1).

3.3.1.8 The Security Subsystem provides the capability for System Administrator to notify all registered users of any identified threats or vulnerabilities relating to any elements of the ROSR (UN8.2).

3.3.1.9 The Security Subsystem provides the capability for registered user to notify all users under Contributor Category of any identified threats or vulnerabilities to a specific application and corresponding benchmark data sets, documentation, etc. (UN8.2).

3.3.1.10 The Security Subsystem provides the capability for weekly website systems scan and sweep to ensure the environments are clear of injected malware or viruses that could transmit malicious viral agent to portal user's computer (UN8.4).

3.3.1.11 The Security Subsystem provides the capability to prevent automated (non- human) user registration.

3.3.1.12 The Security Subsystem provides the capability for encrypted data transfer via HTTPS for protection of private information such as the user registration process via 128-bit SSL certificate.

3.3.1.13 The Security Subsystem provides the capability for recording and storing all system administration access activities in system logs.

3.3.1.14 The DMA OSADP System servers is hosted in a physically secure location

3.3.1.15 The Security Subsystem automatically logs out a user session after 30 minutes of inactivity.

3.3.1.16 The Security Subsystem provides the capability to enforce "strong" passwords requirements; passwords rated "medium" or lower can be locked or banned.

3.3.1.17 The Security Subsystem provides the capability to enforce immediate lock down for at-risk users, which effectively shuts down all system resources access upon activation.

3.3.1.18 The Security Subsystem provides the capability to force users to review site Security Policies every twelve months.

3.4 Functional Requirements

This section describes functional requirements for the systems and subsystems, i.e. "what the system shall do" based on the user requirements. These requirements are organized by the system and subsystem as identified in Figure 1-1. For reference, some requirement statements may have a user need id number in parenthesis, i.e. UN1.1. The full list of User Needs is included in Appendix A.

The User Needs were collected prior to the completion of the Concept of Operations and the Operational Scenarios. In the following text, some references and labeling are reworded to reflect the current environment as they were defined. The rewording maintains the original intention of the User Need statements.

3.4.1 Portal Subsystem

3.4.1.1 The Portal Subsystem shall provide the capability to store and share source code for a hosted application on the portal (UN1.1) and allow registered users to access and download them.

3.4.1.2 The Portal Subsystem shall provide the capability to store and share algorithms for a hosted application on the portal (UN1.2) and allow registered users to access and download them.

3.4.1.3 The Portal Subsystem shall provide the capability to store and share pseudo-code for a hosted application on the portal (UN1.3) and allow registered users to access and download it.

3.4.1.6 The Portal Subsystem shall provide the capability to store and share documentation for a hosted application on the portal (UN1.7) and allow registered users to access and download it.

3.4.1.8 The Portal Subsystem shall provide the capability to store governance document(s) for a hosted application on the portal (UN1.8) and allow registered users to access and download it.

3.4.1.9 The Portal Subsystem shall provide the capability to store data interface standards for a hosted application on the portal (UN1.13) and allow registered users to access and download them.

3.4.1.10 The Portal Subsystem shall provide the capability for registered users to perform searches against open source contents by type (UN13.9).

3.4.1.11 The Portal Subsystem shall provide the capability for visitors to perform searches on the DMA portal public website.

3.4.1.12 The Portal Subsystem shall make the hyperlink to "User Registration" visible on the public website.

3.4.1.13 The system shall provide a method for visitors to communicate with the portal manager. (UN13.10)

3.4.1.14 The Portal Subsystem shall provide registered users the capability to sort project by application category and show related items (UN13.12).

3.4.1.15 The Portal Subsystem shall provide the capability to have a common terminology reference and acronym lookup table accessible by registered users and visitors (UN4.4).

3.4.1.17 The Portal Subsystem shall provide the capability to automatically confirm e-mail address of registering users on the portal via User Registration function (UN8.6).

3.4.1.18 The Portal Subsystem shall provide the capability to host open source applications and source code from other federal agencies per authorization from the Portal Manager (UN12.1).

3.4.1.19 The Portal Subsystem shall provide the capability to recover all portal functionality and contents within 1 week after loss of service (UN8.9).

3.4.1.20 The Portal Subsystem shall provide the capability for meeting Section 508 requirements (UN4.5).

3.4.1.21 The Portal Subsystem shall display usage statistics for shared items including user visit, hits, downloads, and uploads to registered users (UN13.13).

3.4.2 Community Subsystem

3.4.2.1 The Community Subsystem shall provide the capability to allow registered users to share developer community news for a hosted application (UN9.1).

3.4.2.2 The Community Subsystem shall provide the capability to allow registered users to obtain online help (UN9.2) from other community members and the portal administrators.

3.4.2.3 The Community Subsystem shall provide the capability to allow registered users to communicate with project contributors regarding a hosted application via a community discussion forum (UN9.5).

3.4.2.4 The Community Subsystem shall provide the capability to allow registered users to participate in email discussion via community mailing lists (UN9.7).

3.4.2.5 The Community Subsystem shall provide the capability for registered users to collaborate on writing and editing online documents (UN9.9).

3.4.2.6 The Community Subsystem shall provide the capability for registered users to be notified in advance on interesting community events (UN9.17).

3.4.2.7 The Community Subsystem shall provide the capability for registered users to document application-specific resolution for technical issues such as API, objects, libraries and GUI of hosted applications (UN5.4).

3.4.2.8 The Community Subsystem shall provide the capability for registered users to credit and acknowledge the original creator and subsequent contributors of the shared source code or application by displaying their names visibly in association with the shared item, in the ROSR (UN6.4).

3.4.2.9 The Community Subsystem shall provide the capability for registered users to download application source code and associated files, in the ROSR (UN7.3).

3.4.2.10 The Community Subsystem shall provide the capability for registered users to simultaneously upload multiple files into the ROSR (UN7.2).

3.4.2.11 The Community Subsystem shall provide the capability for registered users to submit bug reports specific to each DMA-hosted application into a threaded discussion viewable by other users (UN3.5).

3.4.3 Application Development Subsystem

3.4.3.1 The Application Development Subsystem shall provide the capability to host multiple open source applications during all phases of development (UN11.1)

3.4.3.2 The Application Development Subsystem shall provide the capability to track and control changes to hosted projects' source code (UN2.1).

3.4.3.3 The Application Development Subsystem shall provide the capability to track and control changes to hosted projects' files such as documentation and web pages (UN2.2).

3.4.3.4 The Application Development Subsystem shall provide the capability for authorized users to save, search, share and maintain version control of electronic documents and images of printed documents related to projects e.g., blueprints of street layouts or bridge structure designs (UN2.4).

3.4.3.5 The Application Development Subsystem shall provide the capability to track and control changes to hosted projects' benchmark data and supporting metadata.

3.4.3.6 The Application Development Subsystem shall provide the capability for project members to track issues associated with a hosted application (UN5.2).

3.4.3.7 The Application Development Subsystem shall provide the capability to access hosted application data and files from any location with Internet access (UN11.2). Notes: The intention of this user need statement is make clear that no special network location is required specifically as the source of access to reach the Application Development Subsystem. For some systems, users are required to access them from a particular originating network due to firewall and network access policies.

3.4.3.8 The Application Development Subsystem shall provide the capability to provide information about a hosted application in a Wiki format (UN6.1).

3.4.3.9 The Application Development Subsystem shall provide the capability that requires contributors to include a user's guide for the shared application or source code (UN6.8).

3.4.3.10 The Application Development Subsystem shall provide the capability to collect and display metadata describing the contents and context of a shared item such as purpose of the shared item, means of creation, time and date of creation, creator or author of shared item, and standards used (UN6.9).

3.4.3.11 The Application Development Subsystem shall provide the capability to fork a project or create a similar project based on an existing one, with approval from Portal Manager.

3.4.4 DMA OSADP system

DMA OSADP System will be referred to as "the System" in the following sections.

3.4.4.1 The System shall provide the capability for developers who use shared item(s) to provide updated information on its usage e.g. name of project, role of the application in the project, etc. (UN12.6).

3.4.4.2 The System shall provide the Project Manager the capability to specify the open source agreement for releasing the open source applications (UN1.9) into the ROSR.

3.4.4.3 The System shall provide the capability for visitors to read FAQ (frequently asked questions) with answers (UN9.4).

3.4.4.4 The System shall provide the capability for registered users to read description of applications in ROSR (UN9.4).

3.4.4.5 The System shall create and store application source code and associated files in zip archive format and make them available on ROSR (UN7.4).

3.4.4.6 The System shall provide the capability to recognize and make attribution to application developers and contributors visibly on the application in the ROSR (UN10.1).

3.4.4.7 The System shall provide the capability to recognize and make attribution to contributors of core assets visible on the asset items in the ROSR (UN10.2).

3.4.4.8 The System shall provide the capability to store metadata for a hosted application on the portal (UN1.5).

3.4.4.9 The System shall provide the capability to assign privileges at a granular level to registered users (UN8.7).

3.5 System Operations

These requirements describe the operational aspects of the system.

3.5.1 System Human Factors and Security Risks

Users of the DMA OSADP System are expected to come from geographically-dispersed worldwide locations and can access the DMA OSADP system from anywhere there is Internet access. Not being in a controlled environment of a traditional business office, protected by network firewall and physical security guards, virtual users may unintentionally expose the system environments to a wide range of security risks. To minimize these risks a number of security best practices shall be imposed as requirements. See section 3.3.1 for Security Subsystem requirements.

3.5.2 System Maintainability

3.5.2.1 The System shall provide the capability to patch software defects and upgrade features and functions of the System and Subsystems (UN3.1).

3.5.2.2 The System shall provide the capability for System Administrator to perform website maintenance routines per Portal Manager's direction (UN3.2).

3.5.2.3 The System shall provide the capability to backup the portal and all hosted applications on the portal to offsite server (UN7.1).

3.5.2.4 The System shall provide the capability for System Administrator, in case of content loss, to recover a version of backed up application source code and files to operating condition within 24 hours (UN7.5).

3.5.3 System Reliability

3.5.3.1 The System shall maintain average of 99.9% uptime excluding scheduled downtime for maintenance.

3.5.3.2 The System shall provide registered users the capability to submit technical issue or system bug report with detailed problem description and a severity level of 1-5, via a web browser interface.

3.5.3.3 Downtime of the System shall not exceed 24 hours during a scheduled maintenance period.

3.6 Policy and Regulation

The following requirements consist of non-functional requirements specifically focusing on policy and governance issues of the system.

The IEEE 1362 standard defines operational policies as predetermined management decisions regarding the operations of the proposed system. The following draft operational policies are offered regarding the DMA OSADP System:

3.6.1.1 The user registration process shall require the registrant to agree to the terms and conditions set forth in the user agreement.

3.6.1.2 The system shall provide the capability to invite registered members to join the application development environment.

3.6.1.3 Users shall comply with the portal governance and operation policies.

3.6.1.4 Systems, procedures, and all registered users shall comply with required standards for data privacy.

3.6.1.5 Systems, procedures, and all registered users shall comply with required standards for data security.

3.6.1.6 Systems, procedures, and all registered users shall comply with required standards for quality.

3.6.1.7 Systems, procedures, and all registered users shall comply with required standards for authorized access.

3.6.1.8 Attribution to authors and co-authors of source code shall be shown visibly when possible, next to the person's contribution.

3.6.1.9 The Portal Manager shall enter into a service level agreement (SLA) with the hosting service provider and other computing service providers to ensure prompt and high-quality services and support.

3.7 System Life Cycle Sustainment

This section outlines quality assurance activities, such as review, and measurement collection and analysis that maintain a high quality and operational system.

3.7.1 System Operational Statistics

3.7.1.1 The System shall provide the capability of collecting system statistics regarding usage, performance and user access.

3.7.1.2 The System shall provide System Administrator the ability to review and analyze collected system statistics on usage, performance and user access.

3.7.2 Maintenance Routines

3.7.2.1 System Administrator shall be allowed to perform:

- Daily log review for security and system functionality issues
- Daily user submitted reports and requests review
- Daily review of system usage and analytic reports including user login activity
- Annual system review including reports of system capacities and functionality

3.7.2.2 System scheduled maintenance downtime notice shall be announced 15 days in advance

3.7.2.3 Emergency system shutdown shall be broadcasted to all users via email and on portal public news bulletin.

Chapter 4. Interface Requirements

These requirements describe the subsystems will be interfacing with one another and how the users will interact with it.

The system will not be built from ground up but rather it will be integrated from existing software components with several enabling technologies. Subsystems of the DMA OSADP shall be tightly integrated based on the three subsystem environments as discussed in Figure 2-1. The Portal Subsystem will be the foundation for integrating other software solutions and components onto it.

The focus of this section will be mainly on the user interface with the system.

4.1 User Interface

4.1.1 Web Browsers

4.1.1.1 The DMA OSADP System shall support the following four most popular Internet browsers including Microsoft Internet Explorer, Mozilla Firefox, Safari, and Chrome, and shall stay compatible with at least the latest two versions of the browser releases. (UN13.8).

4.1.2 System Administrator Access Path

4.1.2.1 The DMA OSADP System shall provide System Administrator a special access path for accessing the back-end of the system instead of going through the typical user login page. This access path provides additional security protection.

4.2 System Interface

4.2.1 Developer's System Connectivity

4.2.1.1 The System shall provide developers the ability to connect to the Application Development Environment via web browser.

Chapter 5. Traceability Matrix

5.1 System Requirements to User Needs Mapping Matrix

For tracking the requirements, the matrix below correlates the system requirements described in sections 3 and 4 of this document with user needs and operational use cases identified in previous tasks, shown in Appendices A and B below.

Items in User Needs ID column emphasized in bold are **Must Have** or **Essential** user needs, while the items with regular format are **Nice to Have** or **Desirable** ones.

User requirements in the matrix are hyperlinked with User Needs and Use Cases in the appendices for ease of reference. By clicking on a hyperlink ID, reader will be shown the text of the referred item in the document. The linkage only shows possible correlation between the user requirement statements to a related discussion of the feature or capability, and not necessarily the detailed discussion of the identified requirement. Those items with no correlation in the User Needs ID and User Case ID columns indicate that they are newly added and have not been discussed in previous documents.

Table 5-1. SyRS Matrix Mapping to User Needs and Use Cases

SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.2	**PERFORMANCE REQUIREMENTS**	-	-	
3.2.1.1	The Community Subsystem shall provide the capability to support a minimum 100 concurrent users.		UC2.2, UC3.2, UC3.3	IEEE
3.2.1.2	The Community Subsystem shall provide initially the capability to host at minimum 40 concurrent applications and associated documents in the ROSR, with the ability to scale up storage capacity to accommodate additional applications.		UC2.4, UC2.5, UC3.9, UC4.1	IEEE
3.2.1.3	The Application Development Subsystem shall provide scalable computing resources including CPU, memory, network access and bandwidth, data storage capacity, etc within 5 working days after the request is formally submitted.		UC4.9, UC4.10	IEEE
3.3	**SECURITY REQUIREMENTS**	-	-	
3.3.1	**Data Security**	-	-	
3.3.1.1	The Security Subsystem shall provide the capability to immediately detect, eliminate or quarantine viruses from infected uploaded items before storing them into the ROSR.	**UN5.3**	UC4.1	
3.3.1.2	The system shall be upgraded to include all critical security patches within 5 business days after they are available.		UC4.1	IEEE
3.3.1.3	The Security Subsystem shall provide the capability for Portal Manager to review and approve all content added to the ROSR.	**UN8.5**	UC4.1	
3.3.1.4	The Security Subsystem shall provide System Administrator the capability to see login history for users of the portal.	UN8.8	UC1.3, UC1.6, UC1.7, UC2.1	

SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.3.1.5	The Security System shall provide the capability to prevent unauthorized access into computers and computer networks via all access points with strong security validation and authentication.	UN8.3	UC4.1, UC4.7	
3.3.1.6	The Security Subsystem shall provide the capability to comply with PCI Security Standard Council recommendations and security best practices.		UC4.1, UC4.7	IEEE
3.3.1.7	The Security Subsystem shall provide the capability to display an audit trail of modified files and history of major changes to application source code and files.	**UN8.1**	UC3.4	
3.3.1.8	The Security Subsystem shall provide the capability for system administrator to notify all registered users of any identified threats or vulnerabilities relating to any elements of the ROSR.	**UN8.2**	UC4.4	
3.3.1.9	The Security Subsystem shall provide the capability system administrator to notify all users under Contributor Category of any identified threats or vulnerabilities to a specific application and corresponding benchmark data sets, documentation, etc.	**UN8.2**	UC2.6, UC2.7	
3.3.1.10	The Security Subsystem shall provide the capability for weekly website and system scan and sweep to ensure the environments are clear of injected malware or viruses that could transmit malicious viral agent to portal user's computer.	**UN8.4**	UC4.1	
3.3.1.11	The Security Subsystem shall provide the capability to prevent automated (non-human) user registration.		UC1.3	
3.3.1.12	The Security Subsystem shall provide the capability for encrypted data transfer via HTTPS for protection of private information such as the user registration process via 128-bit SSL certificate.		UC1.1, UC1.3, UC1.6, UC1.7, UC2.1	
3.3.1.13	The Security Subsystem shall provide the capability for recording and storing all system administration access activities in system logs.		UC4.1- UC4.11	
3.3.1.14	The DMA OSADP System servers shall be hosted in a physically secure location			IEEE
3.3.1.15	The Security Subsystem shall automatically log out a user session after 30 minutes of inactivity.	UN8.3		
3.3.1.16	The Security Subsystem shall provide the capability to enforce "strong" passwords requirements; passwords rated "medium" or lower can be locked or banned.		UC1.6, UC1.7	IEEE

SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.3.1.17	The Security Subsystem shall provide the capability to enforce immediate lock down for at-risk users, which effectively shuts down all system resources access upon activation.		UC1.6, UC4.11	IEEE
3.3.1.18	The Security Subsystem shall provide the capability to force user to review site Security Policies every twelve months.			IEEE
3.4	**FUNCTIONAL REQUIREMENTS**	**-**	**-**	
3.4.1	**Portal Subsystem**	**-**	**-**	
3.4.1.1	The Portal Subsystem shall provide the capability to store and share source code for a hosted application on the portal and allow registered users to access and download them.	**UN1.1**	UC3.8, UC3.9	
3.4.1.2	The Portal Subsystem shall provide the capability to store and share algorithms for a hosted application on the portal and allow registered users to access and download them.	**UN1.2**	UC3.8, UC3.9	
3.4.1.3	The Portal Subsystem shall provide the capability to store and share pseudo-code for a hosted application on the portal and allow registered users to access and download them.	**UN1.3**	UC3.4- UC3.9, UC4.9	
3.4.1.4	The Portal Subsystem shall provide the capability to store and share benchmark data sets for a hosted application on the portal and allow registered users to access and download them.	**UN1.4**	UC4.10	
3.4.1.5	The Portal Subsystem shall provide the capability to store and share benchmark data sets and associated metadata for a hosted application on the portal (UN1.3) and allow registered users to access and download them.	**UN1.5**	UC4.10	
3.4.1.6	The Portal Subsystem shall provide the capability to store and share documentation for a hosted application on the portal and allow registered users to access and download them.	**UN1.7**	UC3.8, UC3.9	
3.4.1.7	The Portal Subsystem shall provide the capability to store self-contained, self-validating, and executable formal specifications of test cases to be applied to one or more target modules of hosted projects.		UC4.9	
3.4.1.8	The Portal Subsystem shall provide the capability to store governance document for a hosted application on the portal and allow registered users to access and download them.	UN1.8	UC3.8, UC3.9	

SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.4.1.9	The Portal Subsystem shall provide the capability to store data interface standards for a hosted application on the portal and allow registered users to access and download them.	UN1.13	UC3.8, UC3.9	
3.4.1.10	The Portal Subsystem shall provide the capability for registered users to perform searches against open source contents by type.	**UN13.9**	UC2.4	
3.4.1.11	The Portal Subsystem shall provide the capability for visitors to perform searches on the DMA portal public website.		UC1.2	
3.4.1.12	The Portal Subsystem shall make the hyperlink to User Registration visible on the public website.		UC1.3	DOT
3.4.1.13	The system shall provide a method for visitors to communicate with the portal manager.	UN13.10		
3.4.1.14	The Portal Subsystem shall provide online user training and tutorial on how to use the portal in Community and Application Development environment specifically.	UN13.10		
3.4.1.15	The Portal Subsystem shall provide registered users the capability to sort project by application category and show related items.	UN13.12	UC4.1, UC3.3	
3.4.1.16	The Portal Subsystem shall provide the capability to have a common terminology reference and acronym lookup table accessible by registered users and visitors.	UN4.4		
3.4.1.17	The Portal Subsystem shall provide the capability to allow registered users to configure and customize the primary web user interface screen for emphasizing features of interest to them via pre-defined templates.	UN4.6		
3.4.1.18	The Portal Subsystem shall provide the capability to automatically confirm e-mail address of registering users on the portal via User Registration function.	**UN8.6**	UC1.3, UC1.7	
3.4.1.19	The Portal Subsystem shall provide the capability to host open source applications and source code from other federal agencies per authorization from the Portal Manager.	**UN12.1**	UC3.8, UC3.9	
3.4.1.20	The Portal Subsystem shall provide the capability to recover, in case of an outage, all portal functionality and contents within 1 week after loss of service.	**UN8.9**	UC4.7, UC4.8	
3.4.1.21	The Portal Subsystem shall provide the capability for meeting Section 508 requirements.	**UN4.5**		

SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.4.1.22	The Portal Subsystem shall display to registered users usage statistics for shared items including user visit, hits, downloads, uploads to registered users.	UN13.13		
3.4.2	**Community Subsystem**			
3.4.2.1	The Community Subsystem shall provide the capability that allows registered users to subscribe for notifications when a specific element of the ROSR is changed.	**UN9.8**		
3.4.2.2	The Community Subsystem shall provide the capability that allows registered users to share developer community news for a hosted application.	UN9.1	UC4.2	
3.4.2.3	The Community Subsystem shall provide the capability that allows registered users to obtain online help from other community members and the portal administrators.	UN9.2	UC1.5	
3.4.2.4	The Community Subsystem shall provide the capability that allows registered users to communicate with project contributors regarding a hosted application via a community discussion forum.	UN9.5	UC2.2	
3.4.2.5	The Community Subsystem shall provide the capability that allows registered users to subscribe to receive email notifications on updates to a hosted application.	UN9.6		
3.4.2.6	The Community Subsystem shall provide the capability that allows registered users to participate in email discussion via community mailing lists.	UN9.7		
3.4.2.7	The Community Subsystem shall provide the capability for registered users to collaborate on writing and editing online documents.	UN9.9	UC2.2	
3.4.2.8	The Community Subsystem shall provide the capability for registered users to be notified in advance on interesting community events.	UN9.17		
3.4.2.9	The Community Subsystem shall provide the capability for registered users to document application specific resolution for technical issues such as API, objects, libraries and GUI of hosted applications.	UN5.4	UC4.10	

SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.4.2.10	The Community Subsystem shall provide the capability for registered users to credit and acknowledge the original creator and subsequent contributors of the shared source code or application by displaying their names visibly in association with the shared item, in the ROSR.	UN6.4	UC4.5	
3.4.2.11	The Community Subsystem shall provide the capability for registered users to download application source code and associated files, in the ROSR.	**UN7.3**	UC4.2, UC2.5	
3.4.2.12	The Community Subsystem shall provide the capability for registered users to simultaneously upload multiple files into the ROSR.	UN7.2	UC3.9, UC4.1, UC4.3, UC2.5	
3.4.2.13	The Community Subsystem shall provide the capability for registered users to submit bug reports specific to each DMA-hosted application into a threaded discussion viewable by other users. Note: Remove the notion of e-mail based report since this action is authorized only by registered users.	UN3.5	UC2.6	
3.4.3	**Application Development Subsystem**			
3.4.3.1	The Application Development Subsystem shall provide the capability to host multiple open source applications during all phases of development	**UN11.1**	UC2.4, UC2.5, UC3.9	
3.4.3.2	The Application Development Subsystem shall provide the capability to track and control changes to hosted projects' source code.	**UN2.1**	UC3.4- UC3.8	
3.4.3.3	The Application Development Subsystem shall provide the capability to track and control changes to hosted projects' files such as documentation and web pages.	**UN2.2**	UC3.4- UC3.8	
3.4.3.4	The Application Development Subsystem shall provide the capability to save, version control, make searchable and share-able to authorized users, electronic documents and images of printed documents related to projects e.g., blueprints of street layouts or bridge structure designs.	**UN2.4**	UC3.4- UC3.8	

SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.4.3.5	The Application Development Subsystem shall provide the capability to track and control changes to hosted projects' benchmark data and supporting metadata.		UC3.4- UC3.6	DOT
3.4.3.6	The Application Development Subsystem shall provide the capability for project members to create a custom home page for hosted applications through the use of a WYSIWYG editor.	UN4.3	UC3.2	
3.4.3.7	The Application Development Subsystem shall provide the capability for Project Manager to assign defects associated with a hosted application to project members (Developer, Committer, Tester, and Reviewer).	**UN5.1**	UC2.6	
3.4.3.8	The Application Development Subsystem shall provide the capability for project members to track defects associated with a hosted application.	**UN5.1**	UC2.6	
3.4.3.9	The Application Development Subsystem shall provide the capability for project members to track issues associated with a hosted application.	**UN5.2**	UC2.6	
SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.4.3.10	The Application Development Subsystem shall provide the capability to access hosted application data and files from any location with Internet access. Notes: This intention of this user need statement is make clear that no special network location is required specifically as the source of access to reach the Application Development Subsystem. For some systems, users are required to access them from a particular originating network due to firewall and network access policies.	UN11.2		
3.4.3.11	The Application Development Subsystem shall provide the capability to provide information about a hosted application in a Wiki format.	UN6.1		
3.4.3.12	The Application Development Subsystem shall provide the capability that requires contributors to include a user's guide for the shared application or source code.	UN6.8	UC3.3	

SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.4.3.13	The Application Development Subsystem shall provide the capability to collect and display metadata describing the contents and context of a shared item such as purpose of the shared item, means of creation, time and date of creation, creator or author of shared item, and standards used.	UN6.9	UC3.4	
3.4.3.14	The Application Development Subsystem shall provide the capability to fork a project or creating a similar project based on an existing one, with approval from Portal Manager.		UC4.10	
3.4.4	**DMA OSADP system**			
3.4.4.1	The System shall provide the capability for developers who use the shared item to provide updated information on its usage (e.g., name of project, role of the application in the project, etc.).	UN12.6	UC2.6	
3.4.4.2	The System shall provide the Project Manager the capability to specify which open source agreement for releasing the open source applications into the ROSR.	**UN1.9**	UC3.8	
3.4.4.3	The System shall provide the capability for visitors to read FAQ (frequently asked questions) with answers.	UN9.4	UC3.3	
3.4.4.4	The System shall provide the capability for registered users to read description of applications in ROSR.		UC2.4, UC3.1	DOT
3.4.4.5	The System shall create and store application source code and associated files in zip archive format and make them available on ROSR.	UN7.4	UC2.4	
3.4.4.6	The System shall provide the capability to recognize and make attribution to application developers and contributors visibly on the application in the ROSR.	**UN10.1**		
3.4.4.7	The System shall provide the capability to recognize and make attribution to contributors of core assets visibly on the asset items in the ROSR.	UN10.2	UC4.5	
3.4.4.8	The System shall provide the capability to store metadata for a hosted application on the portal.	**UN1.5**	UC4.6, UC4.7	
3.4.4.9	The System shall provide the capability to assign privileges at a granular level to users.	UN8.7	UC4.9, UC4.10	

SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.5	**System operations**	-	-	
3.5.1	**System human factors** (see section 3.3.1)	-	-	
3.5.2	**System maintainability**	-	-	
3.5.2.1	The System shall provide the capability to patch software defects and upgrade system functions of the Portal Subsystem.	**UN3.1**		
3.5.2.2	The System shall provide the capability for System Administrator to perform website maintenance routines per portal manager's direction.	**UN3.2**	UC4.2	
3.5.2.3	The System shall provide the capability to back up the portal and all hosted applications on the portal to offsite server.	**UN7.1**	UC4.6	
3.5.2.4	The System shall provide the capability for System Administrator, in case of content loss, to recover a version of backed up application source code and files to operating condition within 24 hours.	UN7.5	UC4.7	
3.5.3	**System reliability**	-	-	
3.5.3.1	The System shall maintain average of 99.9% uptime excluding scheduled downtime for maintenance.			IEEE
3.5.3.2	The System shall provide registered users the capability to submit technical issue or system bug report with detailed problem description and a severity level of 1-5, via a web browser interface.		UC2.6	DOT
3.5.3.3	The System shall not exceed 24 hours during a scheduled maintenance period.			IEEE
3.6	**Policy and regulation**	-	-	
3.6.1.1	The user registration process shall require the registrant to agree to the terms and conditions set forth in the user agreement.		UC1.3	DOT
3.6.1.2	The system shall provide the capability to invite registered members to join the application development environment.	UN1.8	UC3.9, UC4.2	
3.6.1.3	Users shall comply with the portal governance and operation policies.	UN1.8	UC4.2	

SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.6.1.4	Systems, procedures, and all registered users shall comply with required standards for data privacy.		UC4.10	IEEE
3.6.1.5	Systems, procedures, and all registered users shall comply with required standards for data security.	**UN8.1**, **UN8.2**, **UN8.4**	UC3.5	
3.6.1.6	Systems, procedures, and all registered users shall comply with required standards for quality.		UC3.5	IEEE
3.6.1.7	Systems, procedures, and all registered users shall comply with required standards for authorized access.	**UN8.6**, **UN8.1**, UN8.8	UC1.6, UC1.7, UC2.1	
3.6.1.8	Attribution to authors and co-authors of source code shall be shown visibly when possible, next to the person's contribution.	**UN10.1**, UN10.2	UC4.5	
3.6.1.9	The Portal Manager shall enter into a service level agreement (SLA) with the hosting service provider and other computing service providers to ensure prompt and high-quality services and support.			DOT
3.7	**System life cycle sustainment**	**-**	**-**	
3.7.1	**System operational statistics**	**-**	**-**	
3.7.1.1	The System shall provide the capability of collecting system statistics regarding usage, performance and user access.	UN13.13		
3.7.1.2	The System shall provide System Administrator the ability to review and analyze collected system statistics on usage, performance and user access.	UN13.13	UC4.7- UC4.10	
3.7.2	**Maintenance routines**			

SyRS ID	Description	User Needs ID	Use Case ID	Req. Ref
3.7.2.1	System administrator shall be allowed to perform: Daily log review for security and system functionality issues; Daily user submitted reports and requests review; Daily review of system usage and analytic reports; Annual system review including reports of system capacities and functionality.	**UN7.1**-UN7.5, **UN8.1**-UN8.8	UC4.1-UC4.11	
3.7.2.2	System scheduled maintenance downtime notice shall be announced 15 days in advance to all users via email and on portal public news bulletin.	**UN3.1**, **UN8.9**		
3.7.2.3	Emergency system shutdown shall be broadcasted to all users via email and on portal public news bulletin.	**UN8.9**		
4	**INTERFACE REQUIREMENTS**	**-**	**-**	
4.1	**User interface**	**-**	**-**	
4.1.1	**Web browsers**	**-**	**-**	
4.1.1.1	The DMA OSADP System shall support the following four most popular Internet browsers including Microsoft Internet Explorer, Mozilla Firefox, Safari, and Chrome, and shall stay compatible with at least the latest two versions of the browser releases.	UN13.8		
4.1.2	**System Administrator access path**	**-**	**-**	
4.1.2.1	The System shall provide System Administrator a special access path for accessing the back-end system instead of going through the typical user login page. This access path provides additional security protection.		UC4.1-UC4.11	
4.2	**System interface**	**-**	**-**	
4.2.1	**Developer's system connectivity**	**-**	**-**	
4.2.1.1	The System shall provide developers the ability to connect to the Application Development Environment via web browser.		UC3.1	IEEE

References

A. USDOT Work Order with Statement of Work (SOW) for Dynamic Mobility Applications Open Source Application Development Portal

B. IEEE Standard 1233 - 1998: IEEE Guide for Developing System Requirements Specifications

C. Task 3.1: Open Source Development Web Resources Scan Assessment Report, dated 28 February 2011

D. Task 3.2: Elicited User Needs for Open Source Portal Technical Memorandum, dated 11 March 2011

E. Task 3.3: OSADP Operational Scenarios, dated 26 May 2011

F. Task 3.3: Concept of Operations – Dynamic Mobility Applications Open Source Application Development Portal, date August 05, 2011

G. Open Technology Development Lessons Learned And Best Practices For Military Software, Version 1.0, dated 16 May 2011

Appendix A. DMA OSADP User Needs

The following table represents the 14 capability categories and 64 user needs as a result of the two workshops' outcomes and analyses, deliverable of TASK 3.2: Elicited User Needs for Open Source Portal Technical Memorandum.

The numbering on the left column with bold emphasis indicates a Must Have / Essential user need and non-bold numbering indicates a Should Have / Desirable user need. The order of the nomenclature is translated directly from "Input No." of Task 3.2 deliverable document.

Table A-5-2. OSADP Prioritized Must-Have / Essential & Should-Have / Desirable User Needs

User Need No.	User Need Description
1. Asset and Content Hosting	
UN1.1	Source Code - Capability to store and share source code for a hosted application on the portal
UN1.2	Algorithms - Capability to store and share algorithms for a hosted application on the portal
UN1.3	Algorithmic Statements / Pseudo-code - Capability to store and share pseudo-code and algorithmic statements for hosted projects on the portal
UN1.4	Benchmark Test Data Sets - Capability to store and share benchmark test data sets for a hosted application on the portal
UN1.5	Metadata - Capability to store data about data of hosted applications on the portal
UN1.7	Documentation - Capability to store documentation for a hosted application on the portal
UN1.9	Type of Open Source Agreement - Capability to specify which open source agreement for releasing the open source applications
UN1.6	Test Procedures - Capability to store self-contained, self-validating, and executable formal specifications of test cases to be applied to one or more target modules of hosted projects
UN1.8	Governance Document - Capability to store a governance document for a hosted application on the portal
UN1.13	Data Interface Standards - Capability to store and share data interface standards (e.g., the interface between traffic signal controllers and RSE and/or OBE)
2. Configuration Management	
UN2.1	Source Control - Capability to track and control changes to hosted projects source code
UN2.2	Version Control - Capability to track and control changes to hosted projects files, such as source code, documentation, and web pages
UN2.4	Document Management - Capability to save, version, share, search, and audit electronic documents and/or images of paper documents related to a hosted project

User Need No.	User Need Description
3. Operations & Maintenance	
UN3.1	Software Upgrade / Patches - Capability to patch defects and upgrade functions of the portal software
UN3.2	System Administration - Capability to perform site maintenance by portal administrators
UN3.5	Application Support - Capability for users to submit e-mail-based bug reports specific to each DMA-hosted application into a threaded discussion viewable by other users
4. User Accessibility	
UN4.5	Section 508 Compliance - Capability to meet Section 508 requirements
UN4.3	WYSIWYG Editor - Capability to easily create a custom home page for hosted applications through the use of a WYSIWYG editor
UN4.4	Online Glossary - Capability to have a common terminology reference and acronym lookup table accessible by portal users and visitors
UN4.6	Configurable User Interface - Capability to allow users to configure and customize the primary user interface screen for emphasizing features of interest to them
5. Bug Reporting	
UN5.1	Bug Tracking - Capability to assign and track defects associated with a hosted application
UN5.2	Issue Tracking - Capability for contributors to track issues associated with the application
UN5.3	Virus Protection - Capability to detect, eliminate or at least quarantine viruses from infected uploaded item and sweep site regularly for malware and any planted viruses
UN5.4	Lessons Learned Repository - Capability for users to document application specific resolution for technical issues such as API, objects, libraries and GUI
6. Documentation	
UN6.1	Wiki - Capability to provide information about a hosted application in a Wiki format
UN6.4	Author Attribution - Capability to credit and acknowledge the original creator and subsequent contributors of the shared source code or application by displaying their name visibly in association with the shared item
UN6.8	User's Guide - Capability to require contributors to include a user's guide for the shared application or source code
UN6.9	Metadata and Information - Capability to collect and display metadata describing the contents and context of a shared item such as purpose of the shared item, means of creation, time and date of creation, creator or author of shared item, and standards used
7. Storage and Backup	
UN7.1	Data Backup - Capability to backup the portal and all hosted applications on the portal
UN7.3	Download - Capability to download files related to a hosted application
UN7.2	Mass Upload - Capability for contributors to upload multiple files simultaneously
UN7.4	Zip Archives - Capability to create and store zip archives for a hosted application

User Need No.	User Need Description
UN7.5	Content Mirroring - Capability to have application content recovered with minimum downtime
8. Security	
UN8.1	Audit Trail - Capability to see an audit trail of modified files
UN8.2	User Security Alert - Capability for the portal administrator or contributors to notify all registered users of a specific application of any identified threats or vulnerabilities
UN8.4	Site Sweep - Capability to ensure user that the site is clear of injected malware or viruses that could affect the portal users
UN8.5	Content Approval - Capability to approve all content added to a hosted application
UN8.6	E-mail Verification - Capability to confirm the e-mail address of users registering on the portal
UN8.9	Portal Recovery - Capability for portal to recover, in case of an outage, all its functionality and contents within 1 week after loss of service
UN8.3	Anti-Hacking - Capability to minimize hacking to the system via all access points with strong security validation and authentication
UN8.7	Granular Privileges - Capability to assign privileges at a granular level to users
UN8.8	Login History - Capability to see a login history for users of the portal
9. Collaboration	
UN9.8	Subscriptions - Capability to allow users to subscribe for notifications when documents or code has been changed
UN9.1	Developer Community News - Capability to share developer community news for a hosted application
UN9.2	Online Help - Capability to provide online help
UN9.4	FAQ Management - Capability to have a FAQ section that is easily updated for each hosted application
UN9.5	Public Forum - Capability to communicate with the contributors to a hosted application via a public forum
UN9.6	Public Mailing List - Capability to receive notifications about a hosted application via e-mail
UN9.7	E-mail to Discussion - Capability to contribute directly to a discussion about a hosted application via e-mail
UN9.9	Groupware - Capability to collaborate on documents located on the portal
UN9.17	Update Alert - Capability to notify registered users via e-mail prior to an interesting event taking place
10. Recognition of Contributors	
UN10.1	User Contribution Recognition/Attribution - Capability to provide contributor recognition and attribution for a hosted application
UN10.2	Recognition of Contributors of Core Assets - Capability to provide recognition of contributors of core assets for a hosted application
11. Hosting Options and Associated Costs	
UN11.1	Hosted Applications - Capability to host multiple open source applications during all phases of development

User Need No.	User Need Description
UN11.2	Cloud Hosting Options - Capability to access hosted application data and files from any location
12. Prototype / Demonstration	
UN12.1	Federal Project Repository - Capability to host open source applications and source code from various federal agencies including transit agency programs such as Safety Pilot Model Deployment and DMA applications
UN12.6	Application Usage Update - Capability for developers who use the shared item to provide updated information on its usage (e.g., name of project, role of the application in the project, etc.)
13. Portal Look and Feel	
UN13.9	Robust Search Engine - Capability to search open source portal contents with parameters for targeting specific content types
UN13.8	Major Browser Support - Capability to support multiple major web browsers
UN13.10	User Training - Capability to provide online user training or tutorial on how to use the portal
UN13.12	Category Sort - Capability to sort projects and show related items by application category
UN13.13	Usage Statistics - Capability to show usage statistics for shared items including user visit, hits, downloads, uploads, and other statistical usage information
14. Other	
UN14.2	International Awareness - Capability for user to acknowledge similar or parallel international efforts [not supported initially]
UN14.5	User Profile Integration - Capability to link with user's existing code repositories, user profiles, and reputation systems [not supported initially]

Appendix B. Detailed Operational Use Cases

The following operational use cases were been discussed in section 6.2 of the Concept of Operation document and recited here for reference.

1. User Interaction, Registration, and Login

UC1.1 Operational Scenario: View publicly accessible content

Actors: Unregistered User, Registered User, Contributor, Administrator (collectively referred to as User)

Description: A user reads publically accessible content including getting started information, terms of use information, DMA program history/context information, news articles, and the glossary.

Preconditions: The User has navigated to the system using Internet browser.

Steps:

1. User navigates to the publicly accessible content of interest.

2. User reads desired information.

If the user wishes to view other publicly accessible content, continue from the beginning.

UC1.2 Operational Scenario: Search publicly accessible pages

Actors: Unregistered User, Registered User, Contributor, Administrator (collectively referred to as User)

Description: A user is looking for certain content. The User inputs search criteria into the system to find the desired information.

Preconditions: The User has navigated to the system using Internet browser.

Steps:

1. User inputs the search criteria, which is either a website link selection or a keyword.

2. User views publicly accessible information

UC1.3 Operational Scenario: Register with system

Actors: Unregistered User, System Administrator

Description: An Unregistered User wants to become a Registered User and have access to additional data and/or participate in the community resources provided by the OSADP. The Unregistered User registers on the site to become a Registered User. A System Administrator reviews the Unregistered User's information to make sure the new Registered User is valid. See Figure B-1.

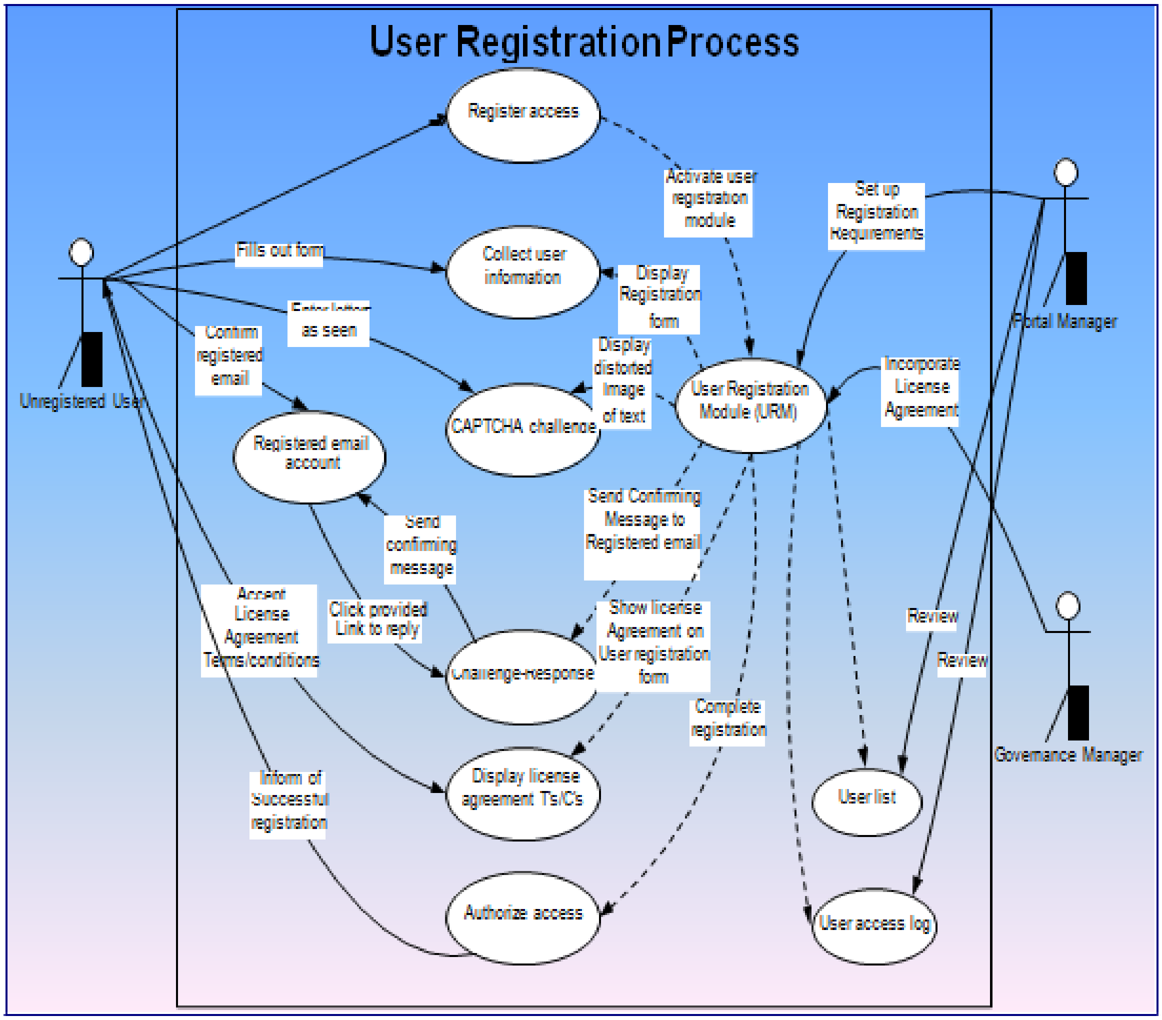
User Registration Process
Register access
Activate user registration module
Set up Registration Requirements
Fills out form
Collect user information
Display Registration form
Enter letter as seen
Confirm registered email
Display distorted image of text
CAPTCHA challenge
User Registration Module (URM)
Incorporate License Agreement
Portal Manager
Unregistered User
Registered email account
Send confirming message
Send Confirming Message to Registered email
Accept License Agreement Terms/conditions
Click provided Link to reply
Challenge-response
Show license Agreement on User registration form
Review
Review
Complete registration
Governance Manager
Inform of Successful registration
Display license agreement Ts/C's
User list
Authorize access
User access log

Figure B-5-1. OSADP User Registration Process

<u>Preconditions</u>: The Unregistered User has navigated to the system using Internet browser.

<u>Steps</u>:

1. Unregistered User navigates to the registration page.
2. Unregistered User reads the terms of use of the site.
3. Unregistered User agrees to the terms of use of the site.
4. Unregistered User enters all mandatory information and, at their discretion, optional requested information. [The specific mandatory and optional information has not been determined. Mandatory information is expected to include: desired username, desired password, valid email address. It may also include full name, organization, organization type, country, and interest with DMA program.]

5. System and Administrator utilize some combination [to be determined] of automated and manual authentication and registration review procedures (e.g., CAPTCHA1 required response to automated email, etc.) to validate registration request.
6. If User passes validation checks, Administrator approves registration and provides email to user.
7. If User fails to authenticate (e.g., User provides an invalid email address or fails to respond to the registration email), Administrator rejects registration.

UC1.4 Operational Scenario: Unauthorized user tries to view content that is not publicly accessible

Actor: Unregistered User

Description: An Unregistered User tries to access information that is not available to the public using non-traditional means. The Unregistered User is denied access to the content.

Preconditions: None.

Steps:

1. Unregistered User attempts to view content that is not publicly accessible by going directly to the URL of the content or accessing the page through non-traditional means.
2. Unregistered User is denied access to the content.

UC1.5 Operational Scenario: Ask a question to Portal Manager

Actors: Unregistered User, Registered User, Contributor, or Portal Manager and Administrator (collectively referred to as User)

Description: A User has a question about information in the OSADP or about the way the OSADP is working. The User sends a message to the Portal Manager, who answers the question or fixes the problem if necessary.

Preconditions: User has navigated to the system using Internet browser.

Steps:

1. User navigates to the appropriate section to send a message to the Portal Manager.
2. User inputs email address, a message subject, and question.
3. Portal Manager reads the question, sends a notification reply that the question has been read and any action that may need to be taken.
4. User reads the Portal Manager's response message.

UC1.6 Operational Scenario: Login to the system

Actors: Registered User, Contributor, Portal Content Manager, or Portal Manager (collectively referred to as User)

[1] CAPTCHA is a type of challenge-response test that attempts to ensure that the response is generated by a human rather than a computer. "CAPTCHA" is a contrived acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart."

Description: The User wants to access the information available at his/her user level in addition to the publically accessible information. The User inputs login information and the system authenticates the User. The User then has access to the information available at user level. See Figure 7.

Preconditions: The User has navigated to the system using Internet browser.

Steps:

1. User navigates to the login area.
2. User enters his login information.
3. User enters his information correctly.
4. User is authenticated.
5. User is given the ability to access data, review his/her profile, and access the community collaboration sections of the DMA OSADP. If the User is a Contributor, the User is also given access to the specific restricted access area within the Application Development. If the user is a Portal Manager, the User is given the ability to create, update, and delete certain content information. If the User is a Portal Manager, the user also receives the ability to modify all Portal Subsystem information.
6. The System Logger records the date, time, and description of the login event.

Extensions:

3a. User enters his/her information incorrectly:

1. The system does not authenticate the login information and displays an error message.
2. Use case resumes at step 2 above.

UC1.7 Operational Scenario: Request a new password

Actors: Registered User, Contributor, Portal Content Manager, or Portal Manager (collectively referred to as User)

Description: The User wants to login to the system but has forgotten password and so requests a new one. The User must provide identification information before the password is reset. The User then creates a new password and logs in.

Preconditions: The User has navigated to the system using Internet browser.

Steps:

1. User navigates to the request new password area.
2. User provides identification information.
3. The system sends a confirming message to the Registered User’s email
4. User clicks on the provided URL that takes user back to the system password reset screen.
5. User is allowed to create a new password.
6. User is logged into the site.

2. Registered User Environment Operations

UC2.1 Operational Scenario: Review and edit profile

Actors: Registered User, Contributor, Portal Content Manager, or Portal Manager (collectively referred to as User)

Description: The User wants to view and edit a user profile. The User inputs the updated profile information and the system saves the changes.

Preconditions: The User has navigated to the system using Internet browser and is logged in to the system.

Steps:

1. If the User is not an Administrator or Portal Manager, the User navigates to personal profile. If the User is an Administrator or Portal Manager, the User has the ability to navigate and access any user's profile.
2. User inputs updated profile information such as email address, password, name, organization, organization type, country, and interest with DMA program.

UC2.2 Operational Scenario: Collaborate with other Registered Users

Actors: Registered User, Contributor, or Portal Manager (collectively referred to as User)

Description: A User wants to share information with or ask other users a question. The User sends a message directly, posts an opinion or question on the discussion forum, or participates in a social network by leaving message or comments on others' wall, so they can then choose to respond and collaborate with the first user. See Figure B1.

Preconditions: Users have navigated to the system using Internet browser and are logged in to the system.

Steps:

1. Registered User navigates to collaboration area.
2. Registered User inputs message information including the title and the actual message. The message could be a question, a request for help, posting a message expressing an idea, contributing to an existing discussion, or information that other Registered Users may find useful.
3. Another Registered User navigates to the collaboration area.
4. The other Registered User views the message.
5. If the other Registered User chooses to respond to the message, the subsequent steps take place:
6. The other Registered User submits a reply message.
7. The first Registered User views the reply. If this user chooses to send a response back, continue from step 5.

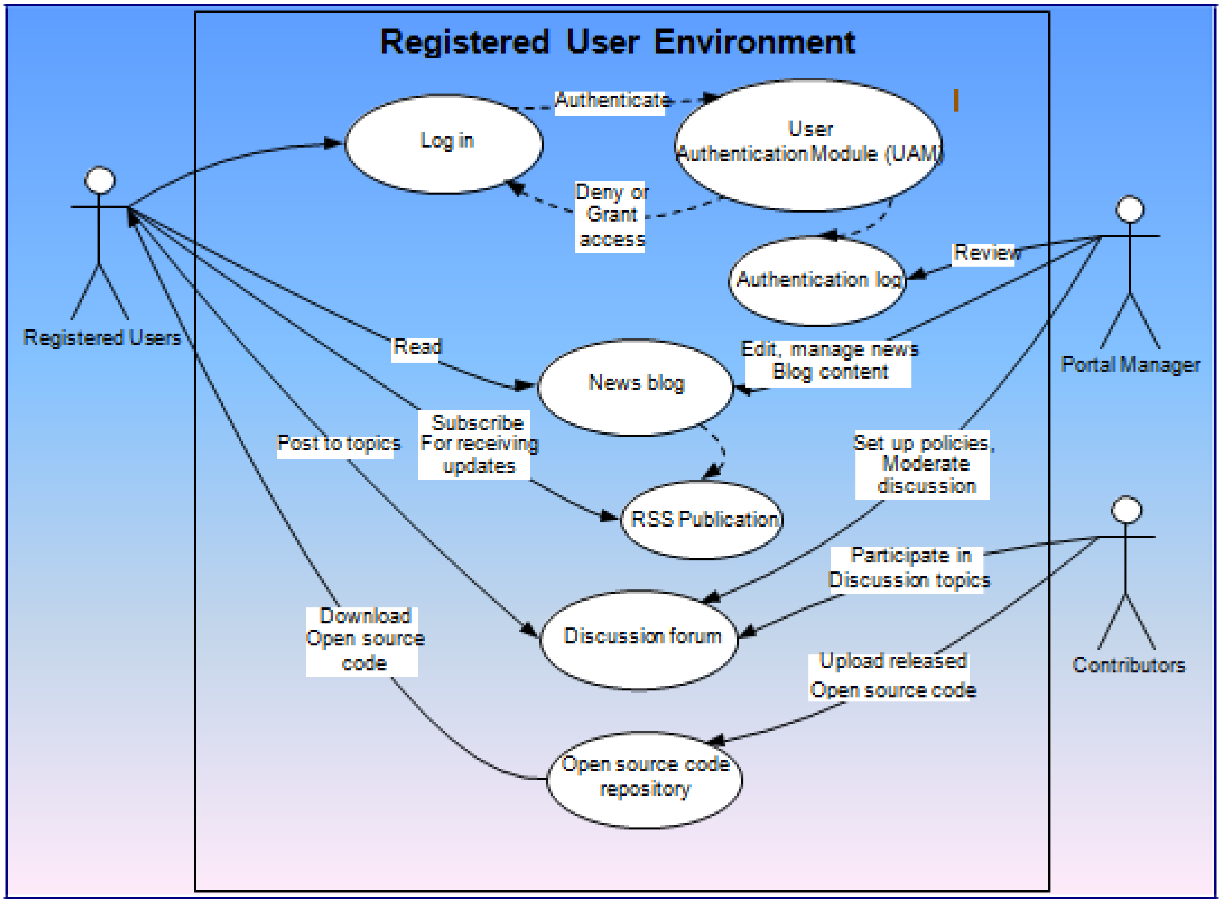
Registered User Environment
Authenticate
Log in
User Authentication Module (UAM)
Deny or Grant access
Authentication log
Review
Registered Users
Portal Manager
Read
News blog
Edit, manage news Blog content
Post to topics
Subscribe For receiving updates
Set up policies, Moderate discussion
RSS Publication
Participate in Discussion topics
Download Open source code
Discussion forum
Contributors
Upload released Open source code
Open source code repository

Figure B-5-2. OSADP Registered User Environment

UC2.3 Operational Scenario: View project information

Actors: Unregistered User, Registered User (collectively referred to as User)

Description: The User navigates to the projects list or news blog entry list and views all of the projects. The User selects a project and views that project's information. See Figure B-2.

Preconditions: User has navigated to the system using Internet browser.

Steps:

1. User navigates to the projects list.
2. User selects a project of interest.
3. User views the information for that project.

If the user wants to view public profile for a Registered User of that project, the subsequent steps take place:

4. If not already logged in, User logs in (Unregistered Users are not allowed to view user profiles).
5. User selects the Registered User whose profile the user wishes to view.
6. User views the profile.

UC2.4 Operational Scenario: Search for and download application from ROSR

<u>Actors</u>: Registered User, Contributor, Portal Content Manager, External Application, or Portal Manager (collectively referred to as User)

<u>Description</u>: The User finds application and wants to download it. If required for the information in question, the User logs in to the system and credentials and permissions are checked against those required for accessing the requested data. If there are no restrictions on access or the user is authenticated and has the required permissions, the user downloads the application archived package and views the data. See Figure B-2.

<u>Preconditions</u>: The User has navigated to the system using Internet browser and is logged in to the system. User has found the information to be downloaded.

<u>Steps</u>:

1. User selects the data or application software to be downloaded.
2. If the User is not logged in and login and/or additional permissions are required for the data in question, the User logs in to the system.
   - The system checks the credentials and permissions of the User
   - If the User is authenticated and has the appropriate permissions, he/she is granted access. If not, an error message is returned to the User.
   - A limited number of attempts are allowed.
3. User accepts terms of the licensing agreement.
4. User downloads the software application or data.
5. User views or stores the data or application software locally.

<u>Extensions</u>:

3a. User does not accept terms of the licensing agreement.

4a. System denies access.

UC2.5 Operational Scenario: Upload enhanced open source code to ROSR

<u>Actors</u>: Registered User, Contributor (collectively referred to as User)

<u>Description</u>: The User downloaded the data or application software and has enhanced the code. User would like to upload the enhanced source code back to the repository. See Figure 8.

<u>Preconditions</u>: User is authorized to download application software or data and make enhancement to the download materials (see *Search for and download application from ROSR*).

<u>Steps</u>:

1. User selects the data or application software area on the repository to upload.
2. If the user is not logged in and login and/or additional permissions are required for the data in question, the User logs in to the system.
   - The system checks the credentials and permissions of the User.

- If the User is authenticated and has the appropriate permissions, access is granted. If not, an error message is returned to the user.
- A limited number of attempts are allowed.

3. User uploads the software application or data.
4. User checks status to confirm that the data or application software has been uploaded successfully.

UC2.6 Operational Scenario: Submit an application bug report

Actors: Registered User, Contributor

Description: The User downloads an application and installs it as instructed. However, the User finds a bug in its application functionality and submits a bug report so that the technical issue can be corrected.

Preconditions: The User is authorized to download application software or data.

Steps:

1. User logs into the portal and navigates to the issue tracker application.
2. User opens a new bug report and describes the symptom of the bug in detail including software version, conditions for the bug to occur, sequence of events leading up to the error, and any system environment that may help replicate the error in the lab.
3. User selects a sensitivity and criticality level for the reported bug and selects type *application bug.*
4. Contributor reviews the bug report, reproduces, and fixes the application bug and tests it.
5. Contributor updates the bug status in the issue tracker application.
6. User later can download and verify the bug fix in the next version release.

UC2.7 Operational Scenario: Submit a portal content error

Actors: Registered User, Portal Manager

Description: The User notices a portal content error and submits a report about it.

Preconditions: User can login to the Registered User Environment

Steps:

1. User logs into the portal and navigates to the issue tracker application.
2. User opens a new portal content error report and describes the error in detail including section or area where the error is found, any side effects, sequence of events leading up to the error, and any system environment that may help replicate the error in the lab.
3. User selects a sensitivity and criticality level for the reported error and selects type *portal content error.*
4. Portal Manager reviews the error report, reproduces, and coordinates with other portal administrative staff to fix the error and test it.
5. Portal Manager updates the portal content error status in the issue tracker application.
6. User later can verify the solution after it is implemented.

3. Application Development Environment Operations

UC3.1 Operational Scenario: Access Application Development Environment

Actors: Contributor, System Administrator, or Portal Manager (collectively referred to as User)

<u>Description</u>*:* The User wishes to update a particular project's information. The User accesses the Application Development Environment and inputs updated project information, which could include the project's reference information and project development code and documents. See Figure B-2.

<u>Preconditions</u>*:* The User has navigated to the system using Internet browser and is logged in to the system.

<u>Steps</u>*:*

1. If the User is a Contributor, the User navigates to the project. If the User is a System Administrator or Portal Manager, the User navigates to any project.
2. If User is not a Contributor, an Administrator, or a Portal Manager, the User can not access the Application Development Environment and will not be able to access in- development projects.
3. If User is a Contributor, User enters Application Development Environment to update project information, which may include any or all of the following: reference information and project development code and documents.
4. Regular Registered Users can not access Application Development Environment.

UC3.2 Operational Scenario: Project meeting

<u>Actors</u>*:* Contributors

<u>Description</u>*:* The Contributors of a particular project hold weekly virtual meeting to get update on project's information. The Project Manager uses an online tool to schedule meetings on specific date and time, conference pass code, and sends out invitation about the meeting to all Contributors of that project. Contributors call in at a predetermined conference number at scheduled time with a pass code to attend the meeting. See Figure 9.

<u>Preconditions</u>*:* Contributors have navigated to the system using Internet browser and are logged in to the system for interactive video meeting tool and have access to a telephone for joining the audio conference. Every project has a web page for posting notes, bulletins, assignment and other project information.

<u>Steps</u>*:*

1. Contributors dial the conference phone number.
2. Contributors open a computer window on their computer and join a video meeting tool.
3. Project Manager leads the meeting.
4. All invited Contributor can participate on meeting topics and discussion.
5. Project Manager captures meeting notes with action items and posts them on project web page.

UC3.3 Operational Scenario: Project collaboration

<u>Actors</u>*:* Contributors

<u>Description</u>*:* As needed, Contributors can collaborate via communication tools such as instant messaging, project technical forum, one-to-one video conference, and computer-to-computer audio/video chat. Through these tools, Contributors can discuss and collaborate on project related efforts.

<u>Preconditions</u>: Contributors have navigated to the system using Internet browser and are logged in to the system that have the collaboration tools enabled for them. See Figure B3.

Steps:

1. Contributor may schedule a session to collaborate with other Contributors, one-to-one or with several others, or the Contributor can attempt to connect directly with another Contributor, impromptu.
2. The other Contributors may respond and participate in technical discussion related to the project.
3. Contributors can brainstorm on an idea, a topic, or help each other on technical topics.
4. All collaboration sessions using these tools will be logged by the system for record purposes.

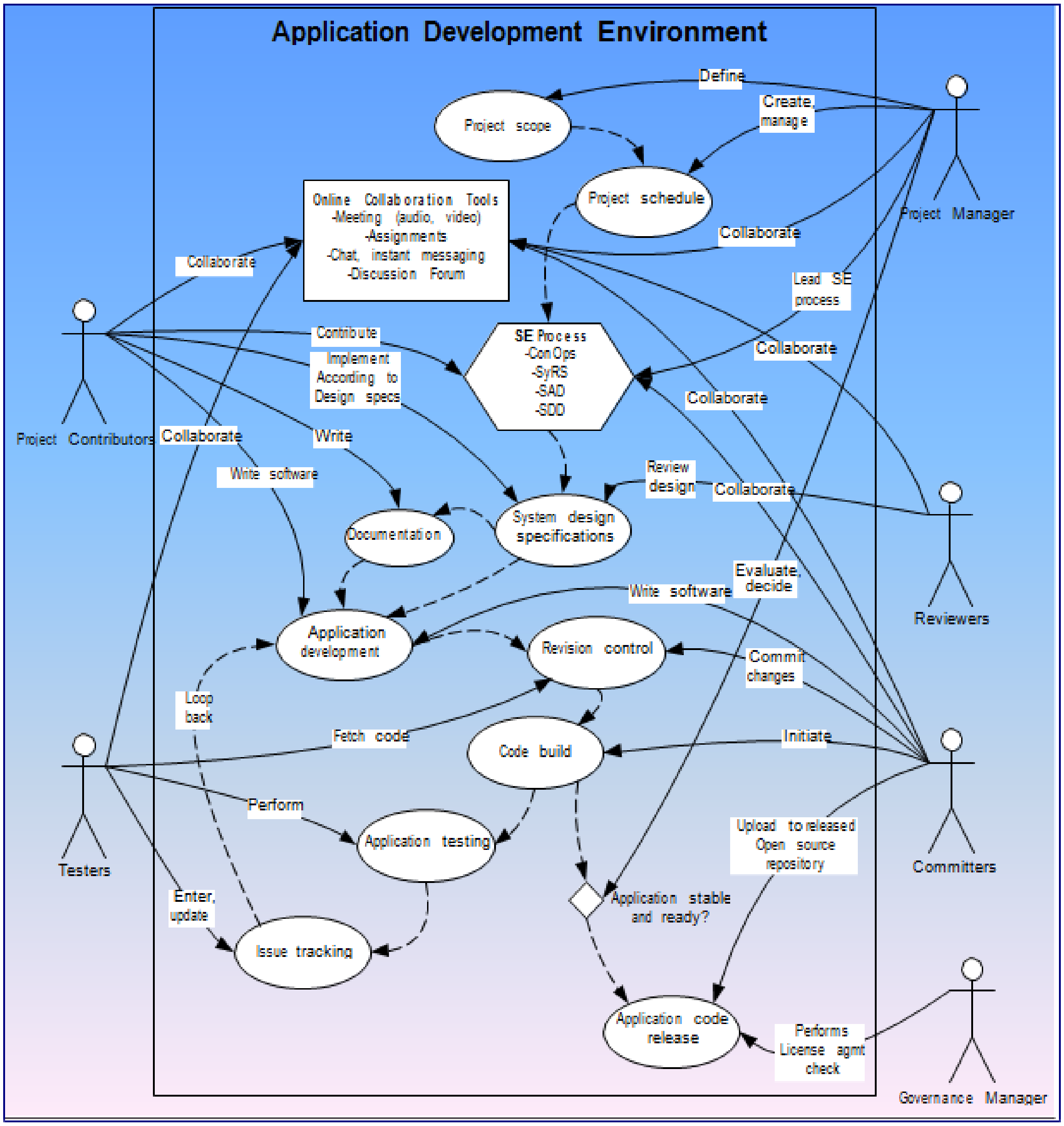

Figure B-3. OSADP Application Development Environment

UC3.4 Operational Scenario: Source control

Actors: Contributors

Description: Contributors in a project save their source code in their individual space. They can use the source control system to check in and check out their in-development code. The revision control system will keep track of the changes and allow the Contributor to make notes about the changes made. See Figure B-3.

Preconditions: Contributors have navigated to the system using Internet browser and are logged in to the system that allows them to navigate to the source control server.

Steps:

1. Contributor develops a source code or a document and wants to save work in provided workspace.
2. As good progress is made on the code or document, Contributor checks in the code or document to a branch in the source control directory.
3. The system automatically increases the version number of the check-in item and prompts the User for entering notes on the changes.
4. The changes are made and the source controlled can be retrieved; Contributor can go back to earlier changes.

UC3.5 Operational Scenario: Code review

Actors: Reviewer and other Contributors

Description: Code review will be performed to ensure quality and assess security vulnerability. Peer Contributors or a qualified Registered User may be promoted to Contributor status for a short duration for performing code review. See Figure 9.

Preconditions: Contributors have navigated to the system using Internet browser and are logged in to the system that allows them to navigate to the source control server.

Steps:

1. Reviewer performs code review.
2. If a qualified Registered User is to be promoted to guest Contributor status, the Project Manager makes request to the System Administrator to change the Registered User's access level to that of a Contributor for a specified period of time which will automatically expire.
3. The guest Reviewer performs code review.
4. Reviewer documents all findings and recommendations in a report to the Project Manager.

UC3.6 Operational Scenario: Code build

Actors: Committer and other Contributors

Description: At certain point in the code development, a software build is needed. The Contributors meet and decide what is to be included in a code build based on its readiness. The Committer works with the other Contributors to make the determination, then commits some code changes to the source control tree trunk for a code build.

Preconditions: Contributors have navigated to the system using Internet browser and are logged in to the system. Contributors have checked in all their relevant changes.

Steps:

1. Each Contributor checks in code or document changes to the source control system.
2. Committer ensures the changes are in the system and copies them into a build directory.
3. Committer orders the build and the system completes the code build.

UC3.7 Operational Scenario: Code testing

Actors: Tester, Project Manager, Committer, other Contributors

Description: The Tester prepares application test plan specific to the system requirements and specifications. The Tester gets approval from Project Manager for the test plan prior to testing. As the code is ready, the Tester will test the code and report bugs and issues. See Figure 9.

Preconditions: The Tester has access to the code to be tested and the targeted system to test them on.

Steps:

1. Tester installs the test code.
2. Tester follows the test plan to verify functionality and features specified in application requirements.
3. Tester documents findings including bugs, issues, and observations.
4. Tester describes the failure conditions so the Contributors can recreate the issues and fix them.

UC3.8 Operational Scenario: Code release

Actors: Tester, Project Manager, Committer, other Contributors

Description: After rounds of testing, including possibly field testing, if the application code passes the tests satisfactorily, the application code will be prepared for release. See **Error! eference source not found.**

Preconditions: Testing completes with satisfactory results.

Steps:

1. Project Manager assesses test results.
2. If they are deemed acceptable, the code will be prepared to be released.
3. Committer oversees the process of preparing the release package, including documentation.
4. Project Manager will document the event and prepare a report to the project sponsor.

Notes: For procured projects, the application development process terminates here. If the application is functional and the program decides to commit the resources, the application will then undergo limited deployment in field testing. Only if the field testing shows the application to be viable and offer transformative benefits, will the application then go to the repository, assuming it is suitable to be offered under an open source license to all the Registered User community.

UC3.9 Operational Scenario: Upload application to ROSR

Actors: Tester, Project Manager, Committer, other Contributors

Description: With the release code, the application will be packaged with documentation and instructions. The process of a User downloading the application will be simulated to ensure the application will have no transmission or installation problems. See Figure 9.

Preconditions: Release code is ready. After DMA program has commissioned a field test and the application is proven viable and offers transformative benefits, it authorizes the application to be released to open source community.

Steps:

1. Project Manager prepares application code release document and announcement.
2. Committer oversees the process of packaging the code.
3. Governance Manager ensures appropriate license information is inserted in the header of application source code files and appropriate documentation is prepared.
4. Committer simulates the process of downloading and installing the application package for detecting any problems with packaging process.
5. If the download and installation test is problem free, the Committer uploads the application package to the ROSR.
6. Registered User community will have access to this application after this point.

UC3.10 Operational Scenario: Evaluate a new Contributor from open source community or other funded projects

Actors: Registered User, Project Manager, Project Sponsor

Description: If a Registered User or a Contributor of another project wishes to collaborate in another project. This process involves an evaluation process to qualify the candidate. See Figure B-3.

Preconditions: The candidate must be a Registered User of the OSADP and have ability to access the OSADP.

Steps:

1. Project Manager identifies and announces project needs to the Registered User community in form of a staffing requisition that outlines the job responsibilities, requirements and expectations.
2. Candidate Registered User or a Contributor of another project responds to the requisition and accepts all terms and agrees to all project requirements through the application form.
3. Project Manager must initiate the project membership qualification evaluation process that evaluates the candidates on case-by-case basis based on possible criteria as follows:
    a. Project specific needs
    b. Candidate's motivation
        1) Becoming a project Contributor
        2) Just checking out open source code
        3) Non-technical, just want to know
    c. Qualification
        1) Skills
        2) Experience
        3) Background

d. Association / Affiliation e. Funding status
e. Sponsored by a federal agency g. No conflict of interest

4. The Project Manager submits proposed candidate to Project Sponsor for final approval.

4. Administrative Tasks

UC4.1 Operational Scenario: Manage uploaded files

Actors: Registered User, Portal Manager, System Administrator

Description: The User wants to add new files to a user upload area. The User inputs the associated file information including the title, description, and categorization. If the User is a System Administrator, assigning categorization includes assigning access to the files. The User inputs the actual file.

Preconditions: The User has navigated to the system using Internet browser and is logged in to the system.

Steps:

1. User inputs file information including: title, description, categorization (if the User is a System Administrator, this includes who has access to the file), and the actual file.
2. The system stores the date, time, and description of the “add file” event as part of the event log in the data store.
3. The system automatically runs anti-virus scan on the uploaded files and quarantines any infected files.
4. If no infection, the system stores the data in the intended location in the ROSR.

Extensions: If the file information input is not valid:

1a. User receives an invalid input error message.

2a. User reenters the file information, if chooses. Repeat from step 2 if the input is valid or from step 5 if it is not.

UC4.2 Operational Scenario: Update portal content

Actors: Portal Manager, Governance Manager, System Administrator

Description: Portal Manager or Governance Manager has updated getting started information, terms of use information, history/context information, or an updated news article, glossary term, or website link to modify in the OSADP. The Portal Manager or System Administrator input the updated content information.

Preconditions: The Portal Manager and System Administrator have navigated to the system using Internet browser and are logged in to the system.

Steps:

1. Portal Manager has ownership and authority over all portal contents.
2. Portal Manager works with Governance Manager for the governance related content.
3. Portal Manager works with Project Managers for project specific contents. Changes in the Application Development Environment are dynamic and frequent and the project Contributors will update these accordingly.

4. Portal Manager works with the System Administrator to change, update who has access to the content, if necessary.
5. The system stores the date, time, and description of the “update content” event as part of the event log in the data store.
6. System Administrator or Portal Manager receives a “content updated” validation message.

<u>Extensions</u>: If the System Administrator or Portal Manager enters invalid information:

3a. System Administrator or Portal Manager receives an error message.
4a. System Administrator or Portal Manager reenters the information. If the new information is valid, continue from step 5. If the information is not valid, continue from step 3a.

UC4.3 Operational Scenario: Promote a Registered User to be a Portal Moderator

<u>Actors</u>: Registered User, Contributor, or Portal Manager

<u>Description</u>: Based on needs, a Registered User may be promoted to a Portal Moderator. The Portal Moderator takes guidance and direction from Portal Manager and enforces portal governance and policies based on assignment. The Portal Manager also can demote the candidate based on performance.

<u>Preconditions</u>: The Portal Moderator has navigated to the system using Internet browser and is logged in to the system. The Portal Manager promotes Registered User to Portal Moderator based on qualifications.

<u>Steps</u>:

1. Portal Manager reviews Registered User’s profile and qualifications.
2. Portal Manager discusses moderator’s responsibilities and expectations with the candidate.
3. If acceptable, Portal Manager changes the Registered User’s access level to that of a Portal Moderator.
4. If the Portal Moderator is not performing the responsibilities to expectations, the Portal Manager may withdraw the Portal Moderator’s access level.

UC4.4 Operational Scenario: Notify misuse of collaboration area so unwanted information can be removed

<u>Actors</u>: Registered User, Portal Moderator, Portal Manager

<u>Description</u>: A User creates a message that is inappropriate or unrelated to DMA program. The Portal Manager receives notification of misuse of the collaboration area or notices the misuse himself. The Portal Manager removes the unwanted message.

<u>Preconditions</u>: The User, Portal Moderator, and Portal Manager have navigated to the system using Internet browser and are logged in to the system.

<u>Steps</u>:

1. User posts an inappropriate or non-DMA program-related message in the collaboration area.
2. If someone informs the Portal Manager of the misuse of the collaboration area, the subsequent steps take place:
    a. Portal Manager receives notification that the collaboration area has been misused.
    b. Portal Manager navigates to the collaboration area or asks a Portal Moderator to take this action.

c. Portal Manager or Portal Moderator views the recent messages, including the inappropriate or non-DMA program-related message.
d. Portal Manager or Portal Moderator deletes the message from the system.
e. Portal Manager or Portal Moderator may also take any or all of the following optional actions:
    1) Notify the Registered User, the originator, that their post has been removed, along with the reason.
    2) Warn the originator that they are at risk for removal from the OSADP if misuse or abuse of the system continues.
    3) Remove the User's registration. The former Registered User is now an Unregistered User.

UC4.5 Operational Scenario: Acknowledge User's contributions

Actors: User, Portal Manager

Description: User contribution of various types is acknowledged and recognized publicly and periodically.

Preconditions: The User completed one of the actions or tasks deemed useful or beneficial to the community.

Steps:

1. User fixes a reported bug in an application and uploads the fix back to repository.

2. Committer verifies that the bug is solved satisfactorily, includes in a major code branch, and acknowledges the User's contribution in the release notes.

3. User's work is recognized in the release notes published with the release of the application version so that the credit is known publicly.

Extensions:

1a. User contributes significantly in a discussion forum on a topic that leads to an innovative solution for a technical issue.
2a. Other Users recognizes the User's contribution.
3a. Portal Manager acknowledges the User's contribution in the weekly blog entry that posted publicly on the Community area.

UC4.6 Operational Scenario: Perform data backup

Actors: Infrastructure Provider, System Administrator

Description: Data backup of the portal environments including the Application Development Environment is performed periodically by the Infrastructure Provider.

Preconditions: The System Administrator works with the Data Provider to specify what data to back up.

Steps:

1. System Administrator specifies data sections and schedule that should be backed up.
2. Infrastructure Provider performs data backup according to the schedule.
3. System Administrator has access to verify the backup data.

UC4.7 Operational Scenario: Perform data restore

Actors: System Administrator, Contributor

Description: Folders of source code and supporting assets get corrupted as a result of virus attack. A Contributor requests that the content of folders get restored from the last backup before the attack.

Preconditions: The System Administrator has access to backup content and can perform the data restore operation.

Steps:

1. Contributor submits the data restore request.

2. System Administrator verifies the request and performs the data restore.

3. The system records this action in the event log.

4. System Administrator notifies the Contributor that the request has been fulfilled.

Extensions:

1a. If a major portion or the entire system needs to be restored, the System Administrator works with the Portal Manager to come up with a data restoration plan including a schedule and a contingency plan.
2a. System Administrator coordinates with the Infrastructure Provider to perform the data restore operation.
3a. The system records this action in the event log.

UC4.8 Operational Scenario: Perform data migration

Actors: System Administrator, Portal Manager

Description: A major portion or the entire system data structure needs to be backed up and moved to a different system.

Preconditions: A complete data backup of the system is available (see *Perform data backup*).

Steps:

1. System Administrator works with the Portal Manager to come up with a data migration plan including a schedule and a contingent action if the restoration did not succeed.
2. System Administrator coordinates with the Infrastructure Provider to stop taking more data files, performs a complete system data backup into external media or alternative backup site according to the data migration plan.
3. System Administrator performs a data restoration operation to place the data into the new system environment and makes appropriate adjustment to allow data to be accessible.
4. The system records this action in the event log.

UC4.9 Operational Scenario: Add new section in the collaboration area

Actors: Portal Manager, System Administrator

Description: The Portal Manager has a reason to add a new section in the collaboration area. Possible reasons include the addition of new data sets, the need for an existing category to be broken into more specific categories, or the addition of similar projects which could benefit from a new collaboration area geared toward those projects. The System Administrator creates a new section per request, and specifies who can access the section.

Preconditions: The System Administrator has navigated to the system using Internet browser and is logged in to the system.

Steps:

1. Portal Manager specifies information about the new section including a title and who can access the section.
2. System Administrator creates the new section based on specified information.
3. System Administrator logs the date, time, and description such as "add new section in the collaboration area" as part of the event log.

UC4.10 Operational Scenario: Add new application development project

Actors: Project Sponsor, Portal Manager, Project Manager, System Administrator

Description: The need for a project has been established. A Project Sponsor from USDOT makes a request to Portal Manager to create a new project on the OSADP. This project may be one of three types: directed management, guided management, or meritocratic management project. The Portal Manager works with System Administrator to set up the project environment.

Preconditions: The USDOT Project Sponsor and Portal Manager have agreed that a new project will be added to the OSADP. The System Administrator, or both Portal Manager and System Administrator have navigated to the system using Internet browser and are logged in to the system. The project requirements and access control policies have been agreed to by the parties. The required information about the new resource has been provided to the Portal Manager including name and contact information of the potential Project Manager and project team members.

Steps:

1. Portal Manager works with the System Administrator to allocate project resources including workspace, webhosting, access to the Application Development Environment systems (e.g., configuration management system, bug tracking application, etc.).
2. Portal Manager works with the System Administrator to enable access and grant permission to the project Contributors of the project based on their roles.
3. Portal Manager updates the portal with information on the new environment.
4. The system stores the date, time, and description of the "add new project" event as part of the event log in the data store.

UC4.11 Operational Scenario: Delete user

Actors: Registered User, Portal Manager, Project Manager, System Administrator

Description: The System Administrator has a reason to delete a User. Reasons to delete a User include: the User misused the collaboration area, the User misused data, or the User no longer needs access to DMA program data. The System Administrator removes the User from the system per the Portal Manager's request.

Preconditions: The System Administrator has navigated to the system using Internet browser and is logged in to the system. Some violation has been noticed or a request to remove a project member comes from a Project Manager.

Steps:

1. Portal Manager assesses the violation and decides whether to remove or delete a Registered User.
2. Portal Manager requests that the System Administrator remove or delete the Registered User.
3. If the request comes from the Project Manager, Portal Manager will request the System Administrator to remove or delete the Registered User.
4. System Administrator navigates to any User's profile.
5. System Administrator deletes the User's profile information and removes the User from the system.

Appendix C - User Class Profiles

Table 5-3. OSADP User Categories and Classes

User Class Profiles	Role Description	Permissions and Capabilities
Unregistered User Category		
Unregistered User	Unregistered users are defined as visitors from the general public who may or may not have an interest in the OSADP. They are not registered with the portal and therefore cannot log in. An Unregistered User can view publically accessible information such as generation content about DMA, as well as other content and documents made available to the general public.	□ Browsing OSADP public web pages □ Viewing and downloading public content that does not require registration □ Completing and submitting online registration form that will be evaluated. Completion of user registration form is a step for qualified Registered User to be considered for additional access as a Registered User.
Registered User Category		
Registered User	Registered Users are users who register with and provide information to the OSADP. In addition to the privileges and access rights of Unregistered Users, Registered Users may have access to additional information and content. Specifically, they have access to resources that require registration.	□ All privileges of Unregistered Users □ Bounded by user agreement terms in the registration process □ Having access to discussion forums, news blog, and announcements □ Ability to participate in online discussions □ Subscribing to news updates □ Reporting bug/error, limitation, and problems with portal content and portal software (e.g., broken links) □ Having access to released source code repository to view, download, test, and make changes to application open source □ Reviewing and updating their personal profile □ Submitting or proposing new and innovative ideas

User Class Profiles	Role Description	Permissions and Capabilities
		□ Reviewing and commenting on other approved projects □ Discussing related project □ Submitting source code or data to the community to use □ Viewing other Registered Users' public profile
Contributor Category		
Project Sponsor	Project Sponsor is a person designated by USDOT to provide oversight for funded projects. The sponsor is involved in the process of funding and giving high- level guidance to the project as it relates to the DMA program. Not expected to be involved intimately with the project at a detailed level, the Project Sponsor interfaces with the Project Manager for project related status and updates.	□ Representing USDOT as the main contact for the project □ Approving funding and resources □ Providing guidance to Project Manager relating to the DMA program overall direction □ Interfacing with Project Manager for status and updates □ Providing final approving for staff addition and reduction proposed by Project Manager □ Providing advisory role in open or meritocratic management projects
Project Manager	A special project member who has project leadership responsibilities including directing application development effort, working with Project Sponsor, and making decisions relating to the well being of project including staffing and resource issues.	□ All privileges of Registered Users □ Ability to vote on project decisions □ Access to all in-development source code repository □ Working with Project Sponsors to secure resource and support □ Providing project leadership and direct application development effort □ Responsible for project management including scope and schedule management □ Leading system engineering process □ Evaluating and deciding on readiness of application □ Collaborating with other Project Managers as necessary □ Access to all project source code and resources

User Class Profiles	Role Description	Permissions and Capabilities
Developer	A Developer is a Contributor who is directly involved in developing the project applications. Developers can play multiple roles.	□ All privileges of Registered Users □ Access to all in-development source code repository □ Participating directly in the application development effort in many different project roles, including designing system components, creating source codes, developing software, troubleshooting and fixing bugs, writing documentation, etc. □ Participating in online discussions □ Performing peer review of codes, provide suggestions, and constructive criticism □ Active Developer may be promoted to a Committer who has specific privileges in version control of codes □ Attending project meetings and discussions and collaborating with other project team members regularly
Committer	A Committer is an active project member who has all privileges that a Developer has with several additional access rights for configuration management, code build, and managing the ROSR.	□ All privileges of Registered Users and of Developer □ Committing code changes in configuration branches to the main trunk in code repository □ Initiating code build and compilation □ Preparing source code for release □ Ability to vote on certain project decisions □ Collaborating with other project team members regularly
Tester	A Tester verifies functionality and features of an application or system per design document and test plan. Testing may occur at various phases of the development process.	□ All privileges of Registered Users □ Access to application or target system □ Documenting bugs and issues and tracking them to resolution □ Building and compiling source code □ Collaborating with project team as required

User Class Profiles	Role Description	Permissions and Capabilities
Reviewer	A Reviewer reviews and provides technical opinions and critical comments on engineering products, including designs, codes and documentation, etc., as needed.	□ All privileges of Registered Users □ Reviewing system engineering and other documents □ Reviewing source code designs, source code, and test results □ Collaborating with project team as required
Administrator Category		
Portal Manager	Portal Manager is responsible for the look- and-feel and content of the portal and the Registered User Environment, including portal news blogs, announcement bulletins, and overseeing the discussion forums	□ All privileges of Registered Users □ Responsible for user experience of General Portal and the Registered User Environment including usability, navigation and search, as well as the overall look-and-feel of these environments □ Producing and editing blog articles □ Managing Portal Moderators of discussion forums and bulletins including removal of unwanted information or messages □ Adding, updating, and deleting data files □ Working with Governance Manager in adding, updating, and deleting terms of use, governance, license, policies and legal related content □ Portal Manager manages all content on the portal, but consults with Governance Manager and Project Managers for their respective content areas □ Working with Project Manager who is responsible for project specific content in the Application Development Environment

User Class Profiles	Role Description	Permissions and Capabilities
Governance Manager	Governance Manager oversees the practice of governance policies and ensures that they are implemented properly and is also responsible for preparation and revision of license agreement, disclaimer, and other legal statements to be posted on the portal.	□ All privileges of Registered Users □ Leading the practice on all governance policies, regulations, compliance, and disclaimer statement, etc. □ Providing oversight and management of risks □ Performing auditing of license agreement terms □ Enforcing proper insertion of open source license statement in source code and monitoring open source content for compliance and compatibility □ Having read-only access to both ROSR and in-development source code repository for inspection purposes
Portal Moderator	Portal Moderator monitors discussion forums, instant chat, social networking, and other collaborating tools in the Registered User community and has ability to remove or delete content, if deemed inappropriate based on governance and portal policies. Portal Manager may promote and demote Registered Users from the community to become Portal Moderators. Portal Moderator may be assigned to use specific communication tools or an area within the community communication forums.	□ All privileges of Registered Users, with Limited read/write access within the community communication tools □ Reporting inappropriate activities to Portal Manager □ Monitoring violations of governance and policies

User Class Profiles	Role Description	Permissions and Capabilities
System Administrat or *If SaaS or PaaS is used, some of these services may be provided.	System Administrator is in charge of installing, supporting, and maintaining servers and other computer systems, and planning for and responding to service outages and other problems. Other duties may include scripting or light programming, project management for systems-related projects, supervising or training computer operators, and being the consultant for computer problems beyond the knowledge of technical support staff.	□ All privileges of Registered Users □ Having system root access and be able to allocate system resources as needed □ Responsibility for system access security □ Adding, removing, and updating user account information, resetting passwords, etc. □ Assigning access rights to project content based on Project Manager's direction □ Ensuring network infrastructure is up and running □ Troubleshooting any reported technical problems □ Analyzing system logs and identifying potential issues □ Installing and maintaining software applications and tools for the Application Development Environment □ Auditing performance of systems and software applications □ Planning system capacities and disaster recovery □ Performing data backups and restoring system from backup after a problem or disaster occurs □ Applying operating system updates and patches □ Monitoring the sharing of data, meta-data, or other information □ Removing unwanted information or messages □ Testing and checking new data sets □ Adding new data sets □ Adding, updating, and deleting history/context information within the portal environment. □ Answering technical queries □ Responsibility for documenting the configuration of the system
Infrastructure Provider Category		

User Class Profiles	Role Description	Permissions and Capabilities
Infrastructure Provider *If IaaS or PaaS is used, this function may be included by the service.	Infrastructure Provider delivers computer infrastructure environment that supports advanced data acquisition, data storage, data management, data integration, data mining, data visualization, and other computing and information processing services distributed over the Internet for enabling OSADP virtual collaboration.	□ Access to the computing resources, including processing capabilities, network resource, data security and data storage system, etc., for provisioning infrastructure services, but no access to the Application Development Environment □ Working with System Administrator to provide requested infrastructure resources and services for OSADP

Appendix D. Glossary of Terms

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) - is a type of challenge-response test used in computing as an attempt to ensure that the response is generated by a person. The process usually involves one computer asking a user to complete a simple test which the computer is able to generate and grade. Because other computers are supposedly unable to solve the CAPTCHA, any user entering a correct solution is presumed to be human. A common type of CAPTCHA requires the user to type letters or digits from a distorted image that appears on the screen.

Cloud Computing - a general term for the computing environment that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that is often used to represent the Internet in diagrams.[2]

Core Assets[3] – refers to all digital contents uploaded or created in the DMA OSADP System, associated with projects, including governance document, type of open source agreement, documentation, metadata, algorithms, methods, source code, benchmark test data sets, supporting metadata, and test procedures, etc.

Federally-Funded Projects - projects funded by federal organizations or agencies, that the application brings benefits and values to transportation mobility program.

Integrated Development Environment (IDE) – is a software development application that brings all of the programmer's tools into one convenient place. In the past, programmers had to edit files, save the files out, run the compiler, then the linker, build the application, and then run it through a debugger separately. Today's IDEs bring editor, compiler, linker and debugger into one place to increase programmer productivity.

Intelligent Transportation Systems (ITS)[4] - improve transportation safety and mobility and enhance American productivity through the integration of advanced communications technologies into the transportation infrastructure and in vehicles. The ITS program encompasses a broad range of wireless and wire line communications-based information and electronics.

Metadata – refers to a structured description of a core asset, specifying one or aspects of the asset such as purpose of the asset, time and date of creation, curator or author, standard used, sponsoring organization, etc.

PCI Security Standards Council - is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for computer account data protection. The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards.

Project members – are individuals working on a project on the DMA OSADP. They have different roles, responsibilities and access privileges. Typical roles in a project may include Project Manager, Developers,

[2] Source: techtarget.com
[3] Source: SOW titled: Dynamic Mobility Applications Open Source Application Development Portal
[4] Source: ITS JPO website under About ITS List of FAQs.

Committers, Tester, Reviewer, etc. More details about these project contributing roles are defined in Appendix C, under Distributor Category.

Service Level Agreement (SLA) – is a contract between a network service provider and customer that specifies, usually in measurable terms, what services the network service provider will furnish. Many Internet service providers provide their customers with an SLA.

Software-as-a-Service (SaaS) - is a software delivery model in which software and its associated data are hosted centrally (typically in the Internet) and are typically accessed by users using a thin client, normally using a web browser over the Internet.

Source Code - is human-readable code saved to a file (or files) that contain instructions for a tool or application. This source code may be written in any number of computer programming languages such as C++, Java...

SSL Certificate - Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security for communications over networks such as the Internet. An SSL certificate (Secure Socket Layer Certificate) is a virtual certificate that is assigned to a domain or hosting account and allows information that has been entered into the website by a user (for example credit card information) to be securely encrypted before it is sent to the receiving.

Appendix E. Acronyms and Abbreviations

ADS	Application Development Subsystem
CMS	Content Management System
COTM	Contracting Officer Technical Manager
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CS	Community Subsystem
DMA	Dynamic Mobility Applications
GUI	Graphical User Interface
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
OBE	On Board Equipment
OS	Operating System
OSADP	Open Source Application Development Portal
PS	Portal Subsystem
ROSR	Released Open Source Repository
RSE	Roadside Equipment
SAIC	Science Applications International Corporation
SLA	Service Level Agreement
SOW	Statement of Work
SyRS	System Requirements Specification
UN	User Needs
URL	Uniform Resource Locator
USDOT	United States Department of Transportation
WYSIWYG	What You See Is What You Get

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487
www.its.dot.gov

FHWA-JPO-17-490

U.S. Department of Transportation