***Version 1.0  
19 August 2013***

**Secure Web Integration Framework   
System/Subsystem Specification   
(SWIF SSS)**

***Code 53223***

*Further dissemination only as directed by Commanding Officer, Space and Naval Warfare Systems Center Pacific,   
San Diego, California 92152-5000, 26 June 2013, or higher authority.*

|  |
| --- |
|  |

**SSC Pacific  
San Diego, CA 92152-5001**

*This page intentionally left blank.*

(U) Record of Changes

*\*A - ADDED M - MODIFIED D – DELETED*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VERSION NUMBER | DATE | NUMBER OF FIGURE, TABLE OR PARAGRAPH | \* A M D | TITLE OR BRIEF DESCRIPTION | CHANGE REQUEST NUMBER |
| Original | 26Jun2013 | All | A | This is the initial version of this specification, developed using the SSC Pacific 5.0 Competency SSS Template dated 09 November 2010, tailored where necessary. Some material still needs additional coordination with stakeholders to finalize the SWIF System Requirements. | N/A |
| 1.1 | 22 July | 3.2 – 3.18 | M | Identified and validated the baseline SWIF requirements with Wanda Lam and Patty Diercks, SSC Pacific |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

(U) Table of Contents

Section Page

*This page intentionally left blank.* ii

(U) Record of Changes iii

(U) Table of Contents iv

(U) List of Figures vi

(U) List of Tables vi

1. (U) SCOPE 1

1.1 (U) Identification 2

1.2 (U) System Overview 2

1.3 (U) Definitions 8

1.4 (U) Document Overview 9

2. (U) REFERENCED DOCUMENTS 10

2.1 (U) Government References 10

2.1.1 (U) Laws, Directives, Instructions and Standards 10

2.1.2 (U) Defense Information Systems Agency (DISA) Reference Material 11

2.1.3 (U) Government Open Source Software (GOSS) Documents 11

2.1.4 (U) Project Documents 12

2.2 (U) Industry References 12

2.3 (U) Other Sources 13

3. (U) REQUIREMENTS 14

3.1 (U) Required States and Modes 14

3.2 (U) SWIF Core Service Requirements 14

3.2.1 (U) System and Common Utilities 14

3.2.2 (U) Visualization 17

3.2.3 (U) Roles and User Account Management 19

3.2.4 (U) Groups 22

3.2.5 (U) Search 22

3.2.6 (U) Workflows and Queues 23

3.2.7 (U) Import/Export 25

3.2.8 (U) Named Areas of Interest 26

3.2.9 (U) Analytic Tools 26

3.2.10 (U) Production 27

3.2.11 (U) Notification 28

3.2.12 (U) Subscription 28

3.2.13 (U) Audit 28

3.2.14 (U) Usage and Performance Analytics 30

3.2.15 (U) System Configuration 30

3.2.16 (U) User Preferences 31

3.2.17 (U) User Interface 31

3.2.18 (U) Database 35

3.2.19 (U) Installation and Configuration 36

3.2.20 (U) Help 37

3.2.21 (U) Deployment 38

3.3 (U) SWIF Application Requirements 38

3.3.1 (U/FOUO) Planning Application 38

3.3.2 (U) Target Folder Application 41

3.4 (U) System Interface Requirements 42

3.4.1 (U) Interface Identification and Diagrams 42

3.4.2 (U) Internal Interfaces 43

3.4.3 (U) External Interfaces 43

3.5 (U) System Internal Data Requirements 44

3.6 (U) Adaptation Requirements 44

3.7 (U) Safety Requirements 44

3.8 (U) Security and Privacy Requirements 44

3.8.1 (U) Security 45

3.8.2 (U) Privacy 50

3.9 (U) System Environment Requirements 51

3.10 (U) Computer Resource Requirements 51

3.10.1 (U) Computer Hardware Requirements 51

3.10.2 (U) Computer Hardware Resource Utilization Requirements 52

3.10.3 (U) Computer Software Requirements 52

3.10.4 (U) Computer Communications Requirements 52

3.11 (U) System Quality Factors 53

3.11.1 (U) Functionality 53

3.11.2 (U) Performance 53

3.11.3 (U) Reliability 54

3.11.4 (U) Maintainability 54

3.11.5 (U) Availability 56

3.11.6 (U) Portability 58

3.11.7 (U) Reusability 59

3.11.8 (U) Testability 59

3.11.9 (U) Usability 59

3.12 (U) Design and Construction Constraints 62

3.13 (U) Personnel-Related Requirements 62

3.14 (U)Training-Related Requirements 63

3.15 (U) Logistic-Related Requirements 63

3.16 (U) Other Requirements 64

3.17 (U) Packaging and Labeling Requirements 64

3.18 (U) Precedence and Criticality of Requirements 65

4. (U) QUALIFICATION PROVISIONS 66

5. (U) REQUIREMENTS TRACEABILITY 107

6. (U) PRECURSOR OF SWIF BASELINE REQUIREMENTS 108

7. (U) NOTES 117

7.1 (U) Acronyms and Abbreviations 117

7.2 (U) Definitions Used in this Document 120

7.3 (U) REQUIREMENTS VERIFICATION Process 121

7.4 (u) Requirements Implementation Order Option 122

(U) List of Figures

Figure Page

Figure 1: (U) SWIF Vision (CV-1) 3

Figure 2: (U) SWIF Operational View (OV-1) 4

Figure 3: (U) SWIF User Interface Operational View (OV-1) 5

Figure 4. (U) Objective SWIF Architecture 6

Figure 5: (U) SWIF Objective Architecture (SVC-1) 7

Figure 6: (U) SWIF External Interfaces 42

Figure 7: (U) Notional Example Representation of Requirement Implementation Order 123

(U) List of Tables

[Table 1. (U) STR Priority Descriptions 55](#_Toc364676372)

[Table 2. (U) Failure Class Definitions 57](#_Toc364676373)

[Table 3. (U) Availability Description 57](#_Toc364676374)

[Table 4. (U) Qualification Provisions for Requirements 66](#_Toc364676375)

This Page Intentionally Left Blank.

# (U) SCOPE

(U) This System/Subsystem Specification (SSS) identifies and establishes the system level requirements for the Secure Web Integrated Framework (SWIF). This SSS further specifies the methods used to ensure that each requirement has been met.

(U) This guide is UNCLASSIFIED in its entirety; pages that contain For Official Use Only content have UNCLASSIFIED//FOR OFFICIAL USE ONLY in the header and the specific paragraphs, tables, images or captions containing the content are marked “**U//FOUO**.”

(U) The format for this specification is based on the SSC Pacific Engineering (5.0) Competency *System/Subsystem Specification (SSS) Template* (TM-TS-07 v1.0) and the SSS Data Item Description (DID; DI-IPSC-81431A; see section 2).

(U) The SWIF Project Manager (PM) assumes responsibility for this document and will update it as required to meet the needs of the target network or program. Updates to this document are performed in accordance with the SWIF Configuration Management Process. Review all changes to this specification in terms of changing requirements the sponsor for concurrence and the Project Manager (PM) so the impact of the changed requirements with respect to cost, schedule, and performance are understood.

(U) The requirements described in this document reflect the functional goals of the objective system. The requirements presented here will be implemented in a phased approach, and will be further refined over a number of spirals. The requirements identified in this document are focused on the objective system. This document is considered a living document that will be modified as evolving requirements reveal additional considerations that must be addressed. Detailed design will be documented in Software Design Descriptions (SDDs), which are expected to further capture derived requirements as well as detailed design. In the event of conflict between this document and the contents of the other SSS documents relative to segment design and development, the SSS shall be considered the governing document. The degree of implementation within each planned spiral is driven by the program’s budget and schedule.

(U) This specification applies to the objective SWIF system baseline. Separate Interface Control Descriptions (ICDs) will address specific requirements pertaining to SWIF external interfaces. Current functional requirements and capabilities of the Unclassified SWIF prototype are included in this document. Other demonstrated versions of the SWIF prototype are not available for review and will not be included in this document. Objective requirements identified in this document may not be implemented for several years or version releases.

(U) This document assumes the reader is familiar with current Web, Enterprise and Database Technologies. Section 2 provides references to these technologies only and does not discuss how these third-party technologies and architectures function.

(U) The following assumptions apply to the system:

* The host site will provide the anti-virus capabilities.
* Only those users with a security clearance equal to or higher than the security level of the server shall be able to access that given system installation.

## (U) Identification

(**U//FOUO**) The *Secure Web Integrated Framework* provides the capability to use a variety of *widgets* or small stand-alone applications that allow users to share specific content dynamically via a Government-secured version of the World Wide Web (WWW). SWIF is initially oriented to supporting the development of military operational planning via restricted access networks.

## (U) System Overview

(**U//FOUO**) SWIF is a Web application with the following objective goals as depicted in Figure 1:

* Provide a security component for use by any widget framework, which includes a database that supports row and attribute level labeling.
* Allow third parties to use SWIF to provide data access to Web-based users via widgets based on the user’s authenticated access (clearance level) and access compartments.
* Provide a common set of services/components that are required by Protection Level 3 (PL-3) systems, common to an enterprise solution.
* Provide services/components that will support mission planning and targeting.
* Provide a core set of widgets to support visualization of enterprise services, mission planning and targeting
* Provide a capability to allow SWIF data to be shared amongst multiple, separate and physically disconnected SWIF deployment installations.

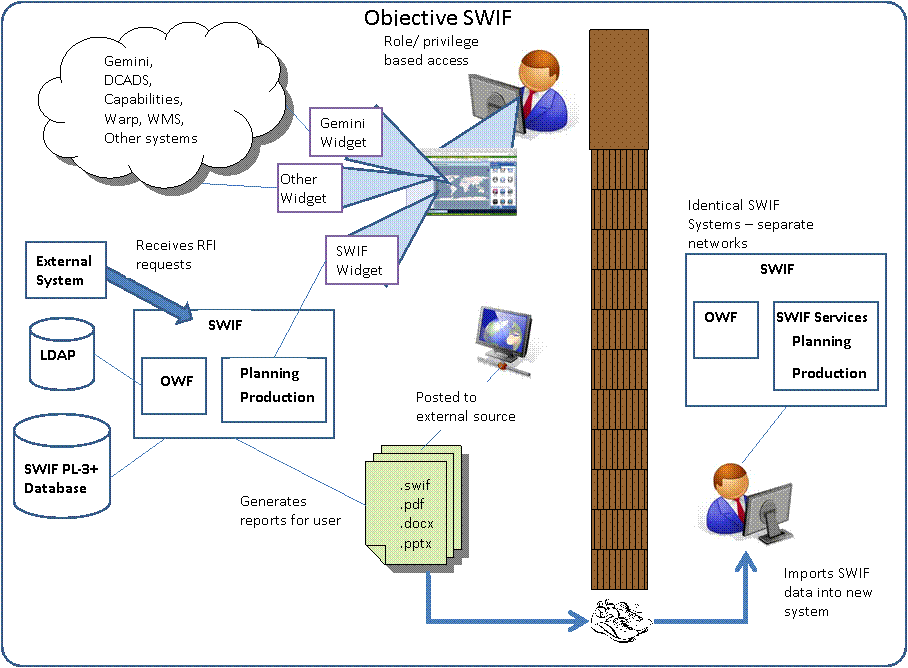


*[Figure is Unclassified]*

1. Figure : (U) SWIF Vision (CV-1)

(U) SWIF provides an additional security infrastructure that allows widgets to meet a target systems security requirements related to Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Attribute Based Access Control (ABAC).

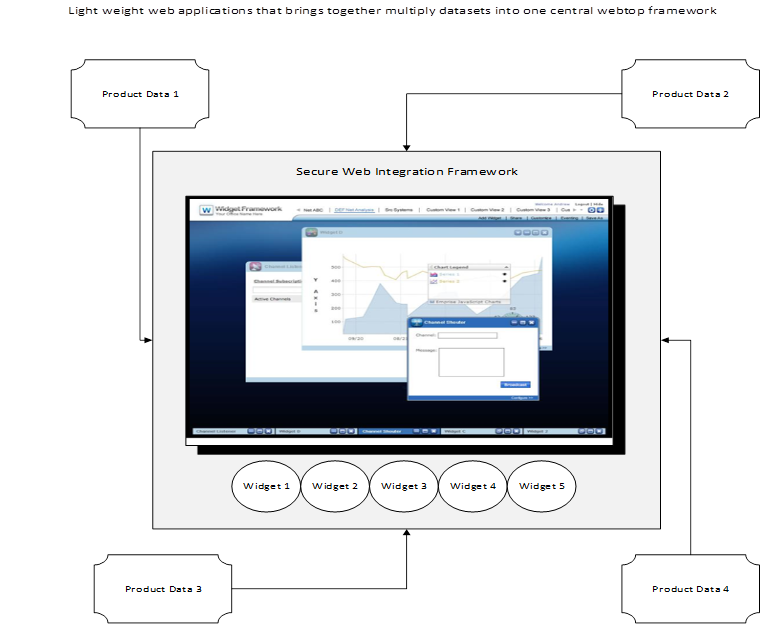
(U) The following figure represents the objective SWIF System:



*[Figure is* ***U//FOUO****]*

Figure : (U) SWIF Operational View (OV-1)

1. (**U//FOUO**) The following figure depicts the objective state of the SWIF capability by showing the Planning Application. Widgets are accessed by users to perform their duties and functions. Each widget will require the user to assign classification to the associated data (used in supporting SWIF Mandatory Access Controls), ensuring users perform planning activities based on their role and security access.



*[Figure is Unclassified]*

1. Figure : (U) SWIF User Interface Operational View (OV-1)
2. (U) SWIF will be designed and developed over a number of spirals. The requirements identified in this document are focused on the objective system. Both this document and the SSDD are living documents that will be modified as detailed design reveals additional considerations that must be addressed. Detailed design will be documented in Software Description Documents which are expected to capture further derived requirements.

(U) The following figures represent the objective SWIF architecture.



*[Figure is* ***U//FOUO****]*

1. Figure . (U) Objective SWIF Architecture



*[Figure is* ***U//FOUO****]*

1. Figure : (U) SWIF Objective Architecture (SVC-1)

(U) Where applicable or required, SWIF design will comply with open source and other standards; custom standards will be implemented only if no other standard exists.

(U) SWIF currently consists of a Web application with REST services exposed for external users. SWIF also provides a JavaScript component that can be used by third-party developers for authentication into the SWIF server, and for setting classification of the data displayed on a Web page.

## (U) Definitions

(U) The following terms and concepts used in this document are provided here to improve the reader’s understanding of the desired system functionality.

* **General User** – A system role whereby the user can access all system functionality that is not administrative in nature and that is authorized for their organization. This will be constrictive in nature and is based on their type of organization. All roles within SWIF are General User roles with the exception of Site Administrators.
* **Privileged User** – A system role whereby the user can access all system functionality, including administration, authorized for the system. Privileged user roles include Site Administrator, Information System Security Manager or Officer (ISSM/ISSO), SSO, and Group Manager.
* **Site Administrator** – A system role whereby the user is responsible for site-level administrative tasks that encompass the host site and that impact all using organizations.
* **SSO** – A system role whereby the user verifies the security clearance of the individual requesting access to the SWIF system. The SSO will verify the requester’s clearance level, compartments, and releasability information. This role is a privileged user role allowing access to security-relevant functions and data, including audit logs.
* **ISSM/ISSO** – A system role whereby the user functions as the activity’s focal point and principal advisor for Information Security (INFOSEC) matters on behalf of the Designated Approving Authority (DAA). The ISSM reports to the DAA and implements the overall INFOSEC program approved by the DAA. An activity may have multiple ISSMs. An ISSO is a system role whereby the user acts on behalf of the ISSM to ensure compliance with the INFOSEC procedures at the operational site or facility. The ISSM is responsible for performing those duties normally performed by ISSOs in the event that no ISSOs are appointed at the particular Command. This role is a privileged user role allowing access to security-relevant functions and data, including audit logs.
* **Group Manager** – A system role whereby the user can perform create, read, update, delete, archive (CRUDA) operations for Groups. Group Managers are privileged users with the authorization to set discretionary access to work products, workflows and queues within the system.
* **Operator** – A system role whereby the user can perform the full scope of CRUDA operations within the system with exception of administrative tasks.
* **External System** – A system role assigned to user accounts that are external systems enabling those systems to access specific SWIF Web services.
* **Viewer** – A system role whereby the user can perform read-only operations within the system with exception of administrative tasks.
* **Tester** – A system role whereby the user can perform test activities and access test tools within the system.
* **System User** – This system role is reserved for internal system component actions only and is not available for assignment to users.
* **Groups** – Two or more system users assembled around a topic of common interest. For SWIF, groups can be used to restrict access to domain-specific programs, system functionality, work products, etc.
* **Capabilities** – A term used to represent various combinations of tools, data, and processes.
* **Work Product** – Deliverable that must be produced to complete a project and achieve its objectives. Within the SWIF architecture, Work products are those deliverable documents generated by users and groups using the domain-specific applications.
* **Entity** – Something that exists as a particular and discrete unit within the system (e.g., object, group/unit, individual, geospatial area).
* **Target Folder** – A folder, hardcopy or electronic, containing target intelligence and related materials prepared for planning and executing action against a specific target.
* **CONOPS** – A verbal or graphic statement that clearly and concisely expresses what the joint force commander intends to accomplish and how it will be done using available resources.
* **Program** – A set of activities with a specific goal that is protected with security protocols providing highly classified information with safeguards and access restrictions that exceed those for regular (collateral) classified information.
* **Domain** – A sphere of activity, concern, or function.

## (U) Document Overview

(U) This SSS is organized into the following sections:

* **Section 1: Scope** — Provides the scope, the identification, and a summary of the contents of the SSS.
* **Section 2: Referenced Documents** — Lists the number, title, revision, and date of all referenced documents.
* **Section 3: Requirements** — Specifies the requirements, including security and privacy, imposed on one or more systems, subsystems, configuration items, manual operations, or other system components to achieve one or more interfaces among these entities.
* **Section 4: Qualification Provisions** — Defines a set of qualification methods and specifies, for each requirement in Section 3, the qualification method(s) to be used to ensure that the requirement has been met.
* **Section 5: Requirements Verification Matrix** — This section is tailored out (not applicable for System Specification).
* **Section 6: Notes** — Contains information of a general or explanatory nature including acronyms and definitions.

# (U) REFERENCED DOCUMENTS

(U) This section lists the specifications, standards, manuals, and other documents, including policy directives, referenced or used as source material for this specification.

## (U) Government References

### (U) Laws, Directives, Instructions and Standards

* Data Item Description, System/Subsystem Design Description (SSDD), DI-IPSC-81431A, 10 August 1999.
* Department of Defense Architecture Framework (DoDAF) Version 2.0.2., <http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf>.
* Joint Operation Planning, Joint Publication 5-0, 11 August 2011, <http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf>.
* Department of Defense Design Criteria Standard Human Engineering, MIL-STD-1472G, 11 January 2012, <http://quicksearch.dla.mil/basic_profile.cfm?ident_number=36903&method=basic>.
* Section 508 of the *Rehabilitation Act of 1973 Technical Guide*, Version 3.30, <http://www.uspto.gov/about/offices/cio/section508/guide_index.jsp>.
* Public Law (P.L.) 107-347, *The E-Government Act of 2002*, Title III, Information Security, Commonly known as the *Federal Information Security Management Act of 2002 (FISMA)*.
* Public Law 100-235, *Computer Security Act of 1987*, 8 January 1988.
* OMB Circular A-123, Management Accountability and Control, 21 June 1995.
* OMB Circular A-130 (Revised), Transmittal Memorandum No. 4 *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, 30 November 2000.
* *Americans with Disabilities Act Accessibility Guidelines for Buildings and Facilities (ADAAG)*, 2004, <http://www.access-board.gov/adaag/about/index.htm>.
* *National Technology Transfer and Advancement Act of 1995*, (Public Law 104-113), 7 March 1996, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.publ113.104.pdf>.
* *Uniform Federal Accessibility Standards (UFAS)*, 1984. <http://www.access-board.gov/ufas/ufas-html/ufas.htm>.
* Chairman of the Joint Chiefs of Staff Instruction CJCSI 6212.01F, *Net-Ready Key Performance Parameter (NR KPP)*, 21 March 2012.
* Department of Defense Manual 5200.0l, *DoD Information Security Program* (Volumes 1-4), January 1997.
* Department of Defense Acting CIO Memorandum, *Clarifying Guidance on Open Source Software (OSS)*, 16 October 2009.
* DoD Directive 8500.1E, *Information Assurance (IA)*, 24 October 2002.
* DoD Instruction 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003, <http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>.
* DoD Instruction 4630.8, 30 June 2004, <http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf>.
* DoD Instruction 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, November 28, 2008.
* Intelligence Community Directive 503 (ICD 503), *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*, 15 September 2008.
* Intelligence Community Directive 710 (ICD 710), *Classification and Control Markings System*, 11 September 2009.
* DCID 6/3, Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, 9 June 1999, administratively updated 1 May 2003.
* DCID 6/6, Director of Central Intelligence Directive (DCID) 6/6, *Security Controls on the Dissemination of Intelligence Information*, 11 July 2001, administratively updated 20 January 2004.
* NIST 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*, <http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf>, August 2009.
* NIST 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, June 2010, <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf>.
* *XML Data Encoding Specification for Information Security Marking Metadata V9* (ISM.XML.V9) 17 July 12 <http://www.dni.gov/files/documents/CIO/ICEA/ISMPublic.zip>.
* Space and Naval Warfare Systems Center, Pacific Instruction (SSCPACINST) 5234.1B, *Project and Systems Engineering Management*, 11 February 2013.

### (U) Defense Information Systems Agency (DISA) Reference Material

(U) Find the following at <http://iase.disa.mil/> (note: these change frequently so specific versions are not included here):

* Security Technical Implementation Guides (STIGs)
* Security Readiness Review Scripts (SRRs)
* Gold Disks
* Security

### (U) Government Open Source Software (GOSS) Documents

* *OZONE Widget Framework Developer’s Guide*, 21 December, 2012 <https://s3.amazonaws.com/org.ozoneplatform/OWF/7-GA/OWF-help-7-GA.zip>
* *OZONE Widget Framework User’s Guide*, 21 December, 2012 <https://s3.amazonaws.com/org.ozoneplatform/OWF/7-GA/OWF-help-7-GA.zip>
* *OZONE Widget Framework Configuration Guide*, 21 December, 2012 <https://s3.amazonaws.com/org.ozoneplatform/OWF/7-GA/OWF-help-7-GA.zip>

### (U) Project Documents

* SWIF System/Subsystem Design Description (SSDD), Version 1.0, 26 June 2013

## (U) Industry References

* *The Java Virtual Machine Specification*, Second Edition Lindholm, Yellin ISBN 0-201-43294-3, copyright 1999.
* *The Java Language Specification*, Third Edition Gosling, Joy, Steele, Bracha ISBN 0-321-24678-01, copyright 2005.
* [*Extensible Markup Language (XML) 1.0 (Fourth Edition)*](http://www.w3.org/TR/2006/REC-xml-20060816/) W3C Recommendation 16 August 2006, Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Eve Maler, François Yergeau eds.
* *ISO/IEC 9075: 1992 Information Technology – Database Language – SQL* with amendment 1, 1996, as modified by FIPS Publication 127-2:1993, Database Language for Relational DBSMSs (Entry level SQL).
* *ISO/IEC 9075-3: 1995 Information Technology – Database Languages – SQL – Part 3: Call-Level Interface (SQL/Call Level Interface (CLI))*.
* OZONE Widget Framework (OWF), <https://www.owfgoss.org/>.
* OZONE Synapse SDK v3.0, <http://widget.potomacfusion.com/pageDisplay/index?menuid=6&pageid=4>.
* *Java Coding Style Guide*,Sun Microsystems, May 2000, <http://developers.sun.com/sunstudio/products/archive/whitepapers/java-style.pdf>.
* OpenSearch v1.1, <http://www.opensearch.org/Specifications/OpenSearch/1.1>.
* OpenSearch Extensions Atom GeoRSS v1.0 Draft 2, <http://www.opensearch.org/Specifications/OpenSearch/Extensions/Geo/1.0/Draft_2>.
* Geography Markup Language (GML) 2.1.2, OpenGIS Implementation Specification, 17 September 2002, OGC Document Number 02-069, <http://www.opengis.org/docs/01-029.pdf>.
* OpenGIS Geography Markup Language (GML) Encoding Specification 3.1.1, 2004-02-07, OGC Document Number 03-105r1, <http://www.opengis.org/docs/01-029.pdf>.
* OpenGIS® Standards and Specifications, Open Geospatial Consortium, Inc., <http://www.opengeospatial.org/standards>.
* OGC Web Processing Service (WPS) standard Version 1.0.0, <http://www.opengeospatial.org/standards/wps>.
* RFC793 Transmission Control Protocol (TCP).
* RFC801 Internet Protocol (IP) Version 4.

## (U) Other Sources

(U) The following sources provided additional material for the creation of this document:

* The deployed Unclassified SWIF prototype, accessible from the SPAWAR RDT&E Network: <https://swif2.spawar.navy.mil/owf>.
* The unclassified SWIF Baseline Software accessible from the SPAWAR RDT&E Network: <https://cmsource.sd.spawar.navy.mil/svn/FAD/trunk>.
* The unclassified SWIF developers notes located at https://cmsource.sd.spawar.navy.mil/confluence/display/ICER.

# (U) REQUIREMENTS

(U) This section contains the requirements for SWIF which consists of two major components: SWIF Services and SWIF Widgets. These two major components are intended to be common and core capabilities within the overall architecture. The requirements for these common and core capabilities are in Section 3.2. In addition to the common and core services, the objective architecture will support services and widgets specific to a domain that can be plugged in and use those core services and widgets. These “application” services and widgets are described in Section 3.3. Please see Figure 1 above for a diagram of the SWIF Objective Architecture.

(U) Each requirement statement in Section 3 is in **bold** font with the following components: abbreviated classification marking [“(U)” or “(U//FOUO)], unique identification number (these IDs are not necessarily in sequential order in this specification, allowing the addition, moving or deleting requirement statements while retaining the unique ID numbers; the numbering indicates where in this specification structure the requirement originally occurred), and requirement statement. Amplifying or explanatory information in normal font follows a requirement statement if necessary.

## (U) Required States and Modes

(U) SWIF will operate in two functional modes: *operational* and *training*. In operational mode, the system may operate in one of three states: fully operational, degraded, or non-operational. The fully operational and training modes are transparent, with each mode operating on separate servers and databases.

(U) The functions and capabilities of SWIF will operate in the same manner in peacetime, crisis, and wartime. There will be no fallback mode or emergency mode designed into the system. During crisis and wartime, however, its communications may be limited to the most critical organizational or geographical areas of need.

(U) SWIF will be fully operational when all critical and operational components are functioning.

(**U//FOUO**) SWIF will be in a degraded state when all critical components are functional and not all of the operational components are functional. In this state, SWIF can provide Planning and Target Folder services. In a degraded state, each working component will operate the same as when all components are operational.

(U) SWIF will be in the non-operational state when one or more of its critical services (e.g., auditing) are not functional. A critical component is one that either is required by policy or is necessary for the correct operation of SWIF. SWIF will not operate when the system’s ability to monitor and report potential security violation capability or any of the accountability services is not operable or is offline.

## (U) SWIF Core Service Requirements

### (U) System and Common Utilities

(U) The following requirement statements apply to the system and common utilities. All data stored and accessed by both system- and domain-specific services will be controlled by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.1.1 The system shall provide access using existing communications architectures.**

(U) These architectures may include a variety of existing wired or wireless networks and broadcasts.

**(U) 3.2.1.2 The SWIF software shall support existing networks that implement the TCP/IP communication protocol.**

**(U) 3.2.1.3 The SWIF server shall support the use of RESTful Web Services for interfacing with external systems.**

**(U) 3.2.1.4 Each system-generated entity shall have a unique identifier.**

(U) This unique identifier can support traceability and linkage.

**(U) 3.2.1.5 The system shall support operations within multiple classified domains.**

**(U) 3.2.1.6 The system shall be able to authenticate user access using external authentication servers.**

(U) This authentication will use the protocols (e.g., Defense Contract Action Data System, DCADS; Active Directory, AD; Open Directory; Lightweight Directory Access Protocol, LDAP) associated with the external authentication servers.

**(U) 3.2.1.7 The system shall comply with the ICD 503 security requirements directed by the DAA.**

(U) ICD 503 defines security requirements for the assigned Protection Level and Levels of Concern for Availability and Integrity.

**(U) 3.2.1.8 The system shall implement security features commensurate with the protection of the targeted deployment network requires.**

**(U) 3.2.1.9 The system shall not allow the same user to be logged into the SWIF server simultaneously using the same browser type.**

**(U) 3.2.1.10 The system shall provide a security service to control access to the system.**

(U) System access control includes providing user authentication and authorization.

**(U) 3.2.1.11 The system shall control access to system functionality based on the user’s role.**

(U)This includes role-based access control (RBAC).

**(U) 3.2.1.12 The system shall control access to system data based on the user’s attributes including clearance.**

(U) The system uses the clearance data to determine row- and cell-based security.

**(U) 3.2.1.13 The system shall implement security features commensurate with Protection Level (PL) 3 identified for the system interfaces for the deployed network.**

**(U) 3.2.1.14 The system shall implement security features commensurate with the Availability Level Basis identified for the system interfaces for the deployed network.**

**(U) 3.2.1.15 The system shall implement security features commensurate with the Integrity Level Basic identified for the system interfaces for the deployed network.**

**(U) 3.2.1.16 The system shall be deployable to multiple container environments with minimal refactoring required.**

(U) This requirement includes application or servlet containers.

**(U) 3.2.1.17 The system shall maintain content replication functionality that is standard with the operating system on a user’s workstation.**

(U) This functionality includes cut, copy and paste.

**(U) 3.2.1.18 The system shall provide for visualization capabilities.**

(U) Required visualization capabilities include those which allow users to display the data stored within the system.

(U) Required visualization capabilities include those which allow users to manipulate the data stored within the system.

**(U) 3.2.1.19 The system shall provide users a customizable display composed of widgets for interacting with data in the data store.**

(U) These widgets will support viewing and manipulating data in the data store.

**(U) 3.2.1.20 The system shall provide a publish/subscribe capability whereby users can register to be notified of significant events related to topics of interest.**

**(U) 3.2.1.21 The system shall provide users the capability to set Discretionary Access to information stored in the system.**

(U) This Discretionary Access can be Group or Individual(s).

**(U) 3.2.1.22 The system shall provide conversion capabilities.**

(U) Conversions include feet-to-meters and vice versa, units of speed, coordinate systems, etc.

**(U) 3.2.1.23 The system shall provide eventing capabilities to support notifications between internal system components.**

**(U) 3.2.1.24 The system shall provide for a status monitoring capability.**

(U) This includes monitoring and reporting system health.

**(U) 3.2.1.25 The system shall provide the capability for Administrators to specify the conditions constituting an anomalous status that merits reporting.**

**(U) 3.2.1.26 The system shall monitor the operational status of all the SWIF components.**

**(U) 3.2.1.27 The system shall generate an audit report to the destinations specified by the Administrator upon detecting an anomalous operational status in any component.**

(U) This action includes recording the anomalous status in addition to generating the report.

**(U) 3.2.1.28 The system shall respond to an anomalous operational status as specified by the Administrator.**

**(U) 3.2.1.29 The system shall collect generated audit data to support security event monitoring.**

**(U) 3.2.1.30 The system shall monitor security events by analyzing collected audit data for anomalous conditions according to ISSO-defined rules to identify potential security violations.**

**(U) 3.2.1.31 The system shall generate an audit report to the destinations specified by the ISSO upon detecting an anomalous security event.**

**(U) 3.2.1.32 The system shall respond to imminent security violations as specified by the ISSO.**

### (U) Visualization

(U) The following requirements describe the system requirements for visualization. These visualization capabilities would support multiple domains and, therefore, are included as common services. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.2.1 The system shall include a user interface (UI) experience that includes widgets for general user functionality.**

**(U) 3.2.2.2 The system shall allow the user to configure widgets into a workspace.**

**(U) 3.2.2.3 The system shall allow the user to perform CRUDA operations for a workspace.**

(U) These user workspace operations are *create*, *read*, *update*, *delete*, *archive* (CRUDA).

**(U) 3.2.2.4 The system shall allow the user to have multiple workspaces.**

**(U) 3.2.2.5 The system shall include a map widget.**

**(U) 3.2.2.6 The map widget shall be capable of displaying system-stored data**

(**U//FOUO**) This stored data includes, for example, Target Folders, Plans, and Capabilities.

**(U) 3.2.2.7 The map widget shall allow the user to generate geospatial shapes.**

(U) These shapes include points, polylines, and polygons to support other system capabilities, such as search.

**(U) 3.2.2.8 The map widget shall be capable of rendering graphic overlays.**

(U) These overlays include raster and vector graphics.

**(U) 3.2.2.9 The system shall include a multidimensional map visualization capability.**

(U) The required map display will be 2D and/or 3D.

**(U) 3.2.2.10 Map-based icons shall be distinguishable by the type of data.**

(U) Data types include *Target*, *Target* *Type*, *Capability*, *Plan*, etc.

**(U) 3.2.2.11 The system shall be able to display map-based icons using a common display standard.**

(U) Map display standards include MIL-STD-2525 and Naval Tactical Data System (NTDS).

**(U) 3.2.2.12 The system shall provide the capability for the user to mouse over an icon displayed on a map overlay to view a summary of information about the icon.**

**(U) 3.2.2.13 The system shall provide the capability for the user to select an icon displayed on a map overlay to view detailed information about the object in a separate window or widget.**

**(U) 3.2.2.14 The system shall support the OpenGIS Web Map Service (WMS) standard for requesting geo-registered map artifacts.**

(U) These geo-registered map artifacts include tiles and overlays.

**(U) 3.2.2.15 The system shall support the ability for a user to select a map server by entering a Map Server URL.**

**(U) 3.2.2.16 The system shall support the OpenGIS Web Features Service (WFS) standard for requesting feature data.**

**(U) 3.2.2.17 The system shall support user selection of a map server from a list of multiple candidate servers for display.**

(U) Candidates include map and overlay servers.

**(U) 3.2.2.18 The system shall be capable of operating widgets within widget frameworks.**

(U) The OZONE Widget Framework (OWF) is an example of a framework which supports widgets (also known as gadgets).

**(U) 3.2.2.19 System widgets shall be capable of operating within different widget frameworks.**

(U) The OZONE Widget Framework (OWF) is an example of a framework which supports widgets (also known as gadgets).

**(U)****3.2.2.20 The SWIF server shall support commonly accepted Web technologies.**

(U) These technologies include patterns and interface protocols such as Asynchronous JavaScript and XML (AJAX), RESTful Web Services.

**(U) 3.2.2.21 SWIF widgets shall interface with the SWIF server using commonly accepted Web technologies.**

(U) These technologies include patterns and interface protocols.

**(U) 3.2.2.22 The system shall provide a widget management environment that allows each user to have at least one workspace.**

(U) This requirement allows each user to have multiple workspaces.

**(U) 3.2.2.23 The system shall include a Search widget to access data.**

(U) This widget allows users to create and execute searches for data stored within and external to the system.

**(U) 3.2.2.24 The system shall include a Search widget that allows users to access stored capabilities.**

(U) This widget allows users to create and execute searches for capabilities within and external to the system.

**(U) 3.2.2.25 The system shall include a Search widget that allows users to search for other users.**

(U) This widget allows users to create and execute searches for other users and their associated attributes in the system (e.g., Security Clearance and access compartments).

**(U) 3.2.2.26 The system shall include a data monitoring widget that allows users to view data feed status.**

**(U) 3.2.2.27 The system shall include a collaboration widget.**

**(U) 3.2.2.28 The system shall include a link analysis widget.**

**(U) 3.2.2.29 The system shall include a graph visualization widget.**

(U) This widget supports charting operations to aid in visualizing data.

**(U) 3.2.2.30 The system shall include a data import widget.**

**(U) 3.2.2.31 The system shall provide a timeline widget.**

**(U) 3.2.2.32 The system shall provide an operations clock tool.**

**(U) 3.2.2.33 The system shall provide a decision matrix widget.**

### (U) Roles and User Account Management

(U) The following subsection contains the system requirements for user account management (UAM). Please reference section 3.8 Security and Privacy Requirements for additional Account Management requirements. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.3.1 The system shall provide a Web-based user interface (UI) to support user account management (UAM) functionality.**

**(U) 3.2.3.2 The system shall provide the capability to use user account privileges to manage user access.**

**(U) 3.2.3.3 The system shall employ user roles that restrict user access to system functionality based on assigned roles.**

**(U) 3.2.3.4 The system shall provide a set of roles to allow users to have system access.**

(U) As a minimum, the system will have the following roles:

* Site Administrator
* Operator
* SSO
* ISSM/ISSO
* Viewer (read-only access)
* External System
* System
* Group Manager

**(U) 3.2.3.5 The system shall allow adding additional roles without requiring a major redesign of the system.**

**(U) 3.2.3.6 The system shall provide the capability to change** **a user’s assigned roles.**

**(U) 3.2.3.7 The system shall provide the capability to reset the passwords for existing user accounts.**

**(U) 3.2.3.8 The system shall notify the user via that user’s account-associated email address when the user’s password has changed.**

**(U) 3.2.3.9 The system shall provide a user account workflow to manage account creation.**

(U) Workflow steps will include security approval, account approval, and activation.

**(U) 3.2.3.10 The system shall support multiple states.**

(U) Acceptable values for account states and statuses include the following (read as State/Status):

* Active/Unlocked
* Active/Locked
* Inactive/Locked
* Inactive/Archived

**(U) 3.2.3.11 User accounts in the system shall be capable of being in only one state at any one time.**

(U) Account state includes the status of the account.

**(U) 3.2.3.12 The system shall retain all user accounts regardless of their current state.**

(U) The system will not delete user accounts from the system for historical purposes based on State/Status.

**(U) 3.2.3.13 The system shall provide the capability for viewing user accounts based on the account state.**

**(U) 3.2.3.14 The system shall assign a unique identifier to each user account.**

**(U) 3.2.3.15 The system shall** **require the use of strong passwords.**

(U) For this system a strong password must contain at least 15 characters, of which there are at least two uppercase letters, two lowercase letters, two numbers, and two symbols. In addition, a strong password cannot be the same as the user’s previous passwords, cannot include the user’s name, and is not your login.

**(U) 3.2.3.17 The system shall reject a password if the user tries to save a password that does not meet the strong password requirement.**

**(U) 3.2.3.18 The system shall lock a user account if the user fails three successive login attempts within a given timeframe.**

**(U) 3.2.3.19 The system shall allow only Administrators to unlock user accounts.**

**(U) 3.2.3.20 The system shall age user account passwords with a maximum allowed usage time limit set as a system configuration item with default to one year (365 days).**

**(U) 3.2.3.21 If a user’s current password has aged beyond three months (90 days), the system shall automatically lock a user account, preventing the user access until the user changes the password for the account.**

**(U) 3.2.3.22 The system shall notify a user each time the user attempts to login if the account password is set to expire, beginning 10 days prior to its expiration.**

**(U) 3.2.3.23 The system shall provide the capability to input specific user information during user account creation.**

(U) User assigned information includes, as a minimum, the following items:

* Login ID
* First name
* Last name
* Organization
* Email address (the required email address type will be driven by the network on which the system is operating, e.g., IC Email if the system is operating at TS/SCI)
* Secure phone number and secure phone type (e.g., VOIP, Red, etc)
* Non-secure phone number

**(U) 3.2.3.24 The system shall not allow the user to access the account during the approval process.**

**(U) 3.2.3.25 The system shall allow the user to change specific values of the user’s account information.**

(U) The user cannot change the login ID, roles, security, account state/status, and account expiration.

**(U) 3.2.3.26 The system shall require all login IDs to be unique.**

**(U) 3.2.3.27 The system shall notify the user, using the user’s email address on file in the account for the network, that a new account has been created for them and is ready for use.**

**(U) 3.2.3.28 The system shall separately notify the user, using the user’s contact email address for the network, of the new temporary account password.**

**(U) 3.2.3.29 The system shall provide a strong password auto-generation capability to assign new passwords for user accounts.**

**(U) 3.2.3.30 The system shall allow the user to use the password auto-generation capability to generate a new password for the user account.**

(U) An Administrator can also use this password auto-generation capability for an account.

**(U) 3.2.3.31 The system shall allow the user to change the user’s system-generated temporary password upon their first login after password reset.**

**(U) 3.2.3.32 The system shall allow the Site Administrator to configure the number of days after creation of a new account the password will expire if the user does not log in.**

**(U) 3.2.3.33 The system shall require all users to revalidate their user account information as part of account renewal in accordance with the renewal time frame within the user account.**

(U) By default, the renewal time frame is 365 days from account activation/reactivation.

**(U) 3.2.3.34 The system shall notify users of their required renewal thirty (30) days prior to their account expiring.**

**(U) 3.2.3.35 The system shall automatically lock user accounts that are not renewed in accordance with the renewal time frame within their user account.**

**(U) 3.2.3.36 The system shall provide the capability for the ISSO to set the renewal time frame for each user account as an individually configurable value.**

**(U) 3.2.3.37 The system shall require account renewal re-approval by revalidation of security clearances with associated accesses by the user’s security officer.**

**(U) 3.2.3.38 The system shall provide a capability dynamically to enforce “least** **privilege” functionality for individual users.**

**(U) 3.2.3.39 The system shall provide the capability to support public key infrastructure (PKI) certificates.**

(U) PKI support includes user accounts and external system interfaces.

**(U) 3.2.3.40 The system shall allow the user to use external credentials for system access.**

External credentials include Passport, PKI.

**(U) 3.2.3.41 The system shall support the concept of an “alias” to hide the true name of the user.**

**(U) 3.2.3.42 The system shall provide the capability to disable system roles.**

(U) This includes for example, if a role is no longer needed

### (U) Groups

(**U//FOUO**) The following subsection describes the system requirements for groups. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements. Groups will not have Mandatory Access Control settings; members may have any clearance type. The system will invoke Mandatory Access Control when the group is associated with other controlled information. For example, if a plan is associated with a Group, and a group member does not have the clearance to view the plan, the group member cannot view the plan, nor will the group member receive any notifications about the plan.

**(U) 3.2.4.1 The system shall provide the capability for users to manage groups of users.**

(U) This management capability includes creating groups.

**(U) 3.2.4.2 The system’s notification capability shall support notifications.**

(U) This notification capability includes both individuals and groups.

**(U) 3.2.4.3 The system shall provide the capability to hide the existence of a group.**

**(U) 3.2.4.4 The system shall allow groups to be composed of individuals from multiple organizations.**

(U) This permits individuals from one or more organizations to comprise a group.

**(U) 3.2.4.5 The system shall allow groups to perform CRUDA operations for a workspace.**

(U) These operations are create, read, update, delete, archive (CRUDA).

### (U) Search

(U) The following subsection describes the system requirements for search. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.5.1 The system shall provide the capability for a user to search for information stored in the SWIF data store.**

**(U//FOUO)** Information in the data store includes CONOPS, Plans, Capabilities, and Target Folders.

**(U) 3.2.5.2 The system shall provide the capability for a user to search for user information residing in data stores external to SWIF.**

(U) External data stores can include Defense Contract Action Data System (DCAD) and Lightweight Directory Access Protocol (LDAP).

**(U) 3.2.5.3 The system shall restrict the ability to search for user information residing in data stores external to SWIF to roles configured by an Administrator.**

(U) In some systems this may mean that all users can search for user information, in other configurations this may be restricted to SSOs and group managers.

**(U) 3.2.5.4 The system shall provide the capability for a user to save search results.**

**(U) 3.2.5.5 The system shall filter search results.**

(U) Criteria for filtering search results includes the submitting user’s access and clearance level.

**(U) 3.2.5.6 The system shall provide a keyword search capability.**

**(U) 3.2.5.7 The system shall provide a map interface for users to conduct geospatial searches.**

**(U) 3.2.5.8 The system shall provide the capability for a user to conduct a geospatial search by entering coordinates.**

**(U) 3.2.5.9 The system shall support multiple coordinate types.**

(U) Supported coordinate types include degrees/minutes/seconds (DMS), decimal degrees, Universal Transverse Mercator (UTM), and Military Grid Reference System (MGRS).

**(U) 3.2.5.10 The system shall provide the capability for exporting search results into a tab delimited ASCII text file.**

**(U) 3.2.5.11 The system shall remove duplicate results from search results prior to displaying the results to the user.**

**(U) 3.2.5.12 The system shall provide the capability for a user to specify the maximum number of results for the system to display per page.**

**(U) 3.2.5.13 The system shall provide the capability, in search results displays, for the user to view the number of total matches found by the search.**

**(U) 3.2.5.14 The system shall sort the entire search results set when data is sorted.**

**(U) 3.2.5.15 The system shall provide the capability for the user, after a result set is returned, to sort the results by selecting the column label of the data fields displayed in the results set.**

(U) Sorting can be in ascending or descending order.

**(U) 3.2.5.16 The system shall allow the user to select results for removal from a search results set.**

(U) The user can select one or more results for removal.

### (U) Workflows and Queues

(U) The following subsection describe the system requirements for workflows and queues. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.6.1 The system shall provide for a workflow capability.**

**(U) 3.2.6.2 The system shall provide for a set of factory-delivered predefined workflows.**

**(U) 3.2.6.3 The system shall provide the capability for Administrators to choose from a set of workflows.**

(U) Workflows range from a simple, expeditious workflow to a more complex collaborative workflow.

**(U) 3.2.6.4 The system shall provide the capability for Group Managers to assign workflow entities to users assigned to their queue as part of the workflow process.**

**(U) 3.2.6.5 The system shall be capable of automatically routing workflow tasks to the appropriate queue based on workflow.**

**(U) 3.2.6.6 The system shall provide the capability to route system work products in workflow on which users can work.**

(**U//FOUO**) The system provides work products (i.e., Plans, CONOPS, Target Folders) to users based on their roles and assignments.

**(U) 3.2.6.7 The system shall provide the capability for a user to view the workflow entity that is in a queue for which the user is assigned.**

**(U) 3.2.6.8 The system shall provide the capability for Administrators to assign Group Managers to queues in a workflow.**

**(U) 3.2.6.9 The system shall provide the capability for multiple users to access a Group’s workflow process simultaneously.**

**(U) 3.2.6.10 The system shall allow entities to move from one activity to the next activity based on the group’s workflow process.**

**(U) 3.2.6.11 The system shall provide notifications to users within a workflow based on status information.**

**(U) 3.2.6.12 The system shall provide the capability for a user to save a workflow.**

**(U) 3.2.6.13 The system shall provide the capability for Group Managers to view their queues.**

**(U) 3.2.6.14 The system shall provide the user with status on the user’s workflow execution processes.**

(U) Workflow execution information includes workflow name, state, and status within the workflow.

**(U) 3.2.6.15 The system shall be capable of storing multiple workflows.**

**(U) 3.2.6.16 The system shall provide the capability for a user to view the workflow history of a workflow entity as it works through the end-to-end workflow process.**

**(U) 3.2.6.17 The system shall provide the capability for users assigned to a workflow to be able to view the Workflow History for all products.**

(U) History includes the following data:

* Identity of individual editing the entity (user id)
* Type of entity submitted
* Unique identifier for the entity submitted
* Action taken during a workflow transition
* Date and time of action
* Successful or unsuccessful transmission (if transmitted)
* Overall classification of the entity(U) 3.2.6.18 The system shall provide the capability for a queue member to set notifications upon receipt of new entities available for work in the member’s assigned queues.

**(U) 3.2.6.19 The system shall provide the capability for a workflow manager to configure queues to support workflow.**

(U) Configuration includes setting up the queues.

**(U) 3.2.6.20 The system shall provide the capability for an Administrator to perform queue management functions.**

(U) Administrator functions include the following:

* Designate a Group Manager
* Assign Queue names
* Link Queues to specific workflow Activities

**(U) 3.2.6.21 The system shall provide the capability for Group Managers to restrict workflow access to specific users.**

(U) Group Managers can restrict access to workflow steps and queues to users who have been granted the role and associated permissions.

**(U) 3.2.6.22 The system shall allow the Group Manager to lock write access to a workflow entity.**

### (U) Import/Export

(U) The following subsection describes the system requirements for import/export. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.7.1 The system shall provide the capability for a user to import data into the SWIF data store.**

(U) Acceptable formats include the following:

* CSV (comma separated value) files
* images
* documents (e.g., Plans, CONOPS)
* SWIF Common Data Model (CDM) format

**(U) 3.2.7.2 The system shall provide the capability for a user to export data from the SWIF data store.**

(U) Acceptable formats include the following:

* CSV files
* Images
* documents (e.g., Plans, CONOPS)
* SWIF CDM format

**(U) 3.2.7.3 The system shall have the capability to receive automated online data ingest** **of sources.**

**(U) 3.2.7.4 The system shall provide the capability to stage ingested data in temporary storage for review before permanent storage.**

**(U) 3.2.7.5 The system shall provide users the capability to set and the accessibility of imported information.**

(U) Accessibility includes the classification of the data.

**(U) 3.2.7.6 The system shall include accessibility information for exporting information.**

Accessibility includes the classification of the data.

**(U) 3.2.7.7 The system shall provide a temporary storage area for imported data that will serve as a “quarantine” area until the data can be reviewed when there is no anti-virus scan available.**

**(U) 3.2.7.8 The system shall provide a capability to convert imported CSV files to SWIF CDM format.**

**(U) 3.2.7.9 The system shall provide a capability that allows imported data to be stored in the SWIF data store.**

**(U) 3.2.7.10 The system shall provide a capability to import Capabilities.**

**(U) 3.2.7.11 The system shall provide a capability to export Capabilities.**

### (U) Named Areas of Interest

(**U//FOUO**) The following subsection describes the system requirements for Named Areas of Interest (NAIs). NAIs are used across the DoD and the Intelligence Community and are a key concept used in Joint Planning; therefore, they are to be included as a core service available for use by any application plugging into the SWIF architecture. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.8.1 The system shall provide the capability for users to perform CRUDA operations for Named Areas of Interest (NAIs).**

(U) These operations are create, read, update, delete, archive (CRUDA).

**(U) 3.2.8.2 The default discretionary access of a Named Area of Interest (NAI) shall be private.**

**(U) 3.2.8.3 The system shall support Named Areas of Interest (NAIs) represented by geodetic coordinates.**

(U) These NAIs can include points, polygons or polylines.

**(U) 3.2.8.4 The system shall provide the capability for users to create a Named Area of Interest (NAI) through text entry of coordinates.**

**(U) 3.2.8.5 The system shall provide the capability for users to create a Named Area of Interest (NAI) by dropping a point or drawing a line or polygon on a geodetic map display.**

**(U) 3.2.8.6 The system shall provide the capability to associate Named Areas of Interest (NAIs) to other entities in the system.**

(**U//FOUO**) Other entities in the system can be Plans, CONOPS, etc.

### (U) Analytic Tools

(U) The following subsection describes the system requirements for analytic tools. These analytic tools can support multiple domains and, therefore, are included as common services. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.9.1 The system shall provide a text analytics capability.**

**(U) 3.2.9.2 The system shall provide a heat map analytic capability.**

**(U) 3.2.9.3 The system shall provide an analysis of competing hypothesis capability.**

**(U) 3.2.9.4 The system shall provide a Geographic Information System (GIS) tool.**

**(U) 3.2.9.5 The system shall provide a statistical analysis tool.**

**(U) 3.2.9.6 The system shall provide predictive models.**

**(U) 3.2.9.7 The system shall provide influence diagramming capability.**

**(U) 3.2.9.8 The system shall provide scientific models.**

**(U) 3.2.9.9 The system shall provide engineering models.**

**(U) 3.2.9.10 The system shall provide system dynamic models.**

**(U) 3.2.9.11 The system shall provide simulation models.**

### (U) Production

(U) The following subsection describes the system requirements for production. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.10.1 The system shall provide the capability to generate products using data stored in the system.**

This includes reports.

**(U) 3.2.10.2 The system shall provide users the ability to develop reports as a result of the analytical operations performed using the domain-specific application.**

(**U//FOUO**) This allows a user to generate and disseminate reports such as Planning reports.

**(U) 3.2.10.3 The system shall provide the capability for users to create customized views that can be made into product templates to suit formatting requirements.**

**(U) 3.2.10.4 The system shall provide the capability for users to generate products in multiple formats.**

(U) Report formats include portable document file (.pdf), Web page, and PowerPoint presentation.

**(U) 3.2.10.5 The system shall generate all products in compliance with classification requirements of the deployment network.**

(U) Classification requirements include Controlled Access Program Coordination Office (CAPCO) or the communications network.

**(U) 3.2.10.6 The system shall provide the capability for users to set the classification of a product.**

(U) This also sets the accessibility of a product.

**(U) 3.2.10.7 The system shall provide the capability for users to set the classification of a product template.**

(U) This also sets the accessibility of a product template.

### (U) Notification

(U) The following subsection describes the system requirements for notifications. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.11.1 The system shall provide a notification capability.**

**(U) 3.2.11.2 The system shall be capable of sending notifications via multiple delivery paths, with email being the default path.**

**(U) 3.2.11.3 The system shall provide the capability for users to set notification preferences.**

**(U) 3.2.11.4 The system shall support the ability to select a notification choice for a supported event via a supported channel.**

(U) Selection choices are enable or disable notification.

### (U) Subscription

(U) The following subsection describes the system requirements for subscription. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.12.1 The system shall provide the capability for a user to set up a feed that displays events relevant to the user’s specified needs.**

**(U) 3.2.12.2 The system shall allow a user to follow a system event.**

(**U//FOUO**) Subscription supports monitoring system events related to a work product (e.g, CONOPS, Plan, Target Folders, Capabilities, Products) or specific individuals associated to a Group; subscription displays significant events about all "followed" items in that user's feed.

**(U) 3.2.12.3 The system shall provide a capability to follow system events.**

(U) These events are activity related to users, entities, and work products.

**(U) 3.2.12.4 Any time a change is made to a followed entity, the system shall make that change appear on the user’s feed.**

**(U) 3.2.12.5 The system shall provide the capability for a user to subscribe to system entities.**

**(U) 3.2.12.6 The system shall provide the capability for a user to subscribe to system work products.**

**(U) 3.2.12.7 The system shall provide the capability for a user to set criteria which, when met, will result in the system notifying the use****r.**

### (U) Audit

(U) The following subsection describes the system requirements for audit. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.13.1 The system shall record significant events in audit records.**

(U) The system shall audit, as a minimum, the following actions/activities (this is meant as *fact of* and does not constitute the capture individual value changes).

* Successful logon and logoff attempts by users.
* Unsuccessful logon and logoff attempts by users
* Account lock-out if user exceeds unsuccessful logon attempt threshold
* New user account creation
* Modification to existing user accounts
* Renewal of existing user accounts
* Successful transmission of information to an external interface
* Unsuccessful transmission of information to an external interface
* Modifications to site system configuration settings
* Received external request
* Disposition of external request

**(U) 3.2.13.3 The system shall provide a Web-based user interface (UI) for viewing audit information.**

**(U) 3.2.13.4 The system shall provide auditing of individual accountability.**

(U) This includes unique identification of each user and the association of that identification with all auditable actions taken by that user.

**(U) 3.2.13.5 The system shall ensure all audit records include information to allow administrators the ability to evaluate the audited event.**

(U) This includes the following information:

* date and time of action (e.g., common network time)
* the system locale of the action (e.g., the IP address the event occurred on, etc.). Note IP will be different when system is operating in a High Availability (HA) configuration.
* the system entity or user (and the user organization) that initiated the action (e.g., user ID, system component, etc.)
* system entity or user (and the user organization) that completed the action (e.g., message recipient, user ID, system component, etc.)
* the resources involved in the action
* the action involved or taken (e.g., account modified, system started, System configuration updated, data transmitted, etc.)
* the success or failure of the action

**(U) 3.2.13.6 The system shall provide protection of the contents of audit trails against unauthorized use.**

(U) This includes unauthorized access, modification, or deletion.

**(U) 3.2.13.7 The system shall provide the capability to allow only those users with the appropriate role access to Audit information.**

(U) This normally is restricted to Administrators.

**(U) 3.2.13.8 The system shall restrict all historical logs in such a manner that they cannot be edited by a general user.**

### (U) Usage and Performance Analytics

(U) The following requirements describe the system’s requirements for usage and performance analytics (UPA). All data stored and accessed by this service shall be controlled by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.14.1 The system shall limit access to usage and performance analytics (UPA) by role.**

(U) General users normally should not have access to UPA metrics.

**(U) 3.2.14.2 The system shall provide a Web-based user interface (UI) to support usage and performance analytics (UPA).**

**(U) 3.2.14.3 The system shall provide the capability for an authorized user to view usage and performance analytics (UPA) information for a specified period****.**

(U) This general information includes the following:

* Number of account requests
* Number of accounts approved
* Number of users who successfully logged in
* Number of login failures
* Number of logins by user
* Number of work products generated overall
* Number of work products generated by user
* Number of work products generated by type
* Amount of bandwidth used in processing web requests and/or external communications (e.g., sending e-mail, etc.)
* Average duration of a user web session (if possible)

### (U) System Configuration

(U) The following requirements describe the system’s requirements for setting and managing configurations. All data stored and accessed by this service shall be controlled by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.15.1 The system shall provide a Web-based user interface (UI) to support System Configuration functionality.**

**(U) 3.2.15.2 The system shall restrict access to application configuration settings to privileged users designated as application administrators.**

(U) This normally is the *Administrator* role.

**(U) 3.2.15.3 The system shall provide the capability for an administrator to set configurations.**

(U) These settings, as a minimum, include the following:

* Configure User Account Management
* Set the system’s time zone; the default time zone normally should be Zulu
* Set the name of the site (installation)
* Reset passwords
* Set the system’s maximum classification
* Enter the location of external authentication servers to be used to verify clearance levels

**(U) 3.2.15.4 The system shall provide the capability for Administrators to set the E-Mail configuration preferences.**

(U) These settings, as a minimum, include the following:

* Establish a Default Originator email address
* Establish a Default E-mail Subject Line
* Specify a Simple Mail Transfer Protocol (SMTP) Server

**(U) 3.2.15.5 The system shall provide the capability for Administrators to set map configuration preferences.**

(U) These settings, as a minimum, include the following:

* List of Map Servers accessible by users
* Icon type (e.g., MIL-STD 2525)
* Number of days in the past to display data
* Entity types to display

### (U) User Preferences

(U) The following subsection describes the system requirements for setting and managing user preferences. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.16.1 The system shall allow a user to configure the user’s preference****s for data display.**

**(U)3.2.16.2 The system shall allow a user to configure the user’s preferences for notifications.**

**(U) 3.2.16.3 The system shall allow a user to update only the user’s own user profile information.**

**(U) 3.2.16.4 The system shall allow a user with the role of Administrator to update user preferences for any user.**

**(U) 3.2.16.5 The system shall provide a Web-based user interface (UI) for viewing user preferences.**

**(U) 3.2.16.6 The system shall allow each user to select the type of map-based icons for the user’s map displays.**

**(U) 3.2.16.7 The system user interface (UI) shall allow a user to configure the user’s preferences for default settings.**

**(U) 3.2.16.8 The system shall allow a group to configure the display preferences that can then be used by members of the group.**

**(U) 3.2.16.9 The system shall allow a user to save the user’s preferences for workspace settings.**

### (U) User Interface

(U) The following subsection describes the system’s requirements for the UI. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.17.1 The system shall provide a browser-based user interface (UI) to execute system functions.**

**(U) 3.2.17.2 The system user interface (UI) presented to the user shall be based on the user’s role.**

**(U) 3.2.17.3 The system’s Web-based user interface (UI) shall not rely upon the browser back button for navigation.**

(U) Although the back button should be supported; all navigation must be supplied via explicit links.

**(U) 3.2.17.4 The system’s Web-based user interface (UI) shall use consistent naming conventions for action buttons.**

Action buttons include *Save*, *Cancel*, *Apply*, *Add*, *Remove*, *Delete*, *Archive*, *Search*, and *Refresh*.

**(U) 3.2.17.5 The system shall support forms with consistent behavior.**

This behavior includes the following:

* Forms shall open with the cursor in the top left entry field.
* Forms shall support the use of the TAB key to move the cursor in a Z pattern from left to right and top to bottom through the fields of the form.
* All form screens shall have a *CLEAR* button on the screen to clear all user entry from the fields of the form.
* All form screens shall have a *SAVE* button on the screen to save the data entered into the fields of the form.
* All form screens shall have *DONE* a button on the screen to exit the form entry process.
* All form screens shall have a *CANCEL* button on the screen to exit the form entry process without saving the information entered since the previous SAVE function was executed.
* Forms shall provide field validation.
* Fields that fail validity checking as a result of user-initiated submission shall result in the system providing a flag for user action to correct the error.

**(U) 3.2.17.6** **The system shall use a CLOSE button (if in view mode) to close the current window.**

**(U) 3.2.17.7 The system shall provide a flag for user action to populate mandatory fields that are not populated.**

**(U) 3.2.17.8 When a field fails validity checking, the system will flag the invalid data values within the template prompting user correction of the invalid data.**

**(U) 3.2.17.9 The system shall allow the selection of a single item obtained from the results of a search, displaying its details in a new window.**

**(U) 3.2.17.10 The system shall allow the selection of the details of associated entities.**

This selection supports displaying the details.

**(U) 3.2.17.11 If a user entry must be one of several defined items, then the system shall present the user with the list of items from which to select the entry.**

**(U) 3.2.17.12 The system shall have a consistent layout of the fields regardless of the mode for pages with more than one mode.**

An example is a page with *Create*, *Edit*, and *View* modes.

**(U) 3.2.17.13 The system user interface (UI) shall provide the capability for the user to associate entities using a drag-and-drop metaphor.**

**(U) 3.2.17.14 The system shall use display tags that indicate the presence of mandatory field in a consistent manner for all user-entered fields within the system.**

**(U) 3.2.17.15 The system shall use a consistent markup format on user interface (UI) features to indicate when a selection is not available to the user.**

(U) The selection may include a function or a field.

**(U) 3.2.17.16 The system shall contain an automatic timeout capability.**

(U) This function will be such that if the user has been inactive for a set (configurable) period, the system will automatically log the user out.

**(U) 3.2.17.17 The system shall provide error message windows with consistent behavior.**

(U) This behavior includes the following:

* Display error messages in a scrollable window.
* The user shall be able to select the fields available for display in the error window.
* The user shall be able to select the field for sorting the display in the error window.
* The user shall be able to select the sort order for the display in the error window.

**(U) 3.2.17.18 The system shall provide Save functionality within the browser-based user interface (UI).**

(U) This behavior includes the following:

* User selection of Save shall save the current values in all fields to the database; the only validation done is that which is necessary to successfully get the data into the database (i.e., data format and non-nullables, but no business rules).
* Provide a *Save As* (copy) capability for the various work products.

**(U) 3.2.17.19 The system shall support field validation.**

Field validation will occur only during Create or Edit mode and will be consistent in validating all fields for data format and business rules but will not save, submit to workflow, or finalize.

**(U) 3.2.17.20 The system shall display tags that indicate the presence of mandatory fields in a consistent manner for all user data entry capabilities within the system.**

**(U) 3.2.17.21 Use a consistent format and markup on user interface features to indicate when a function/field is not available to the user.**

**(U) 3.2.17.22 The system shall provide for the following general behavior for the system’s work products.**

(U) A work product may only be opened in edit mode if the current user has work product generation privileges, has the lock, and it has not already been finalized.

(U) Operations which are not appropriate given the current status are disabled. Possible actions for a particular work product are the following:

* *Lock and Review* – if the work product is currently unlocked
* *Unlock* – if the product is currently locked by the current reviewer
* *Recall and Review* – if the product is currently locked by a different reviewer, requests lock release, once finalized, allows the recaller to open the work product
* *Finalize* – finalizes and locks the work product.

**(U) 3.2.17.23 The system shall provide a defined set of capabilities for the user interface (UI) to support Search.**

(U) At a minimum, the UI will provide the following capabilities:

* Allow the user to choose from a predefined list of fields those fields to be included in the search.
* Allow the user to include fields in the results table that are not part of the search.
* Provide the capability in free-text fields to use Boolean indicators.
* Ability to use quoting characters to allow multi-word searches.
* Within free-text fields, the ability to use a wildcard symbol.
* Allow the user to choose sorting results by any one of the fields included in the search or in the results.
* Execution of a search shall cause a results table to be displayed.
* The user shall be able to specify the number of results to include on each results page.
* The user shall be allowed to jump immediately to any result page.
* The user may click on any metadata column header of any column except the one upon which it is currently sorted, to re-sort the results by that column.
* The results of a particular search shall be isolated, i.e. while paging through results, any newly created products shall not appear in the list. Products that were modified since the search executed shall still display the old metadata, until a new search is executed.
* Due to search isolation, the time the search was executed shall be displayed in the results page.
* Hovering over a result row shall result in a tool-tip style popup that displays additional useful metadata about the product that was not included as a column in the result table.
* The user shall be allowed to select one or more search results and export them to a tab delimited ASCII text file.
* From the results table, a *refine search* operation shall take the user back to the search screen and re-populate all the search fields that generated the current result.
* From the results table, a *new search* operation shall take the user back to the search screen with all search fields returned to their default values.

**(U) 3.2.17.24 The system shall provide the ability to color-code settings in the user interface (UI).**

This behavior can include the severity (level) value of the audit table records displayed to the user or communications status.

**(U) 3.2.17.25 The system shall provide a feedback mechanism to the user to indicate the system is processing the user-requested action if the transaction requires more than two (2) seconds to respond.**

**(U) 3.2.17.26 The system’s Web-based user interface (UI) shall not require Java to be installed in the user’s browser.**

**(U) 3.2.17.27 The system’s Web-based user interface (UI) shall not use Java applets.**

### (U) Database

(U) The following subsection describes the system requirements for the database.

**(U) 3.2.18.1 The system shall incorporate data storage capabilities that support transactions using, at a minimum, a v3 Java Database Connectivity (JDBC) driver****.**

**(U) 3.2.18.2 The system database shall support protection of classified data.**

This includes both row and attribute level protection/classification.

**(U) 3.2.18.3 When accessing a non-SQL database, the system shall incorporate a relational database that supports transactions.**

**(U) 3.2.18.4 The system database shall permit internal application connections for the purposes of managing system information.**

This includes managing and manipulating applicable system information.

**(U) 3.2.18.5 The system database shall provide the capability to store audit information.**

**(U) 3.2.18.6 The system database shall provide the capability to store work product information.**

**(U) 3.2.18.7 The system database shall provide the capability to store entity information.**

**(U) 3.2.18.8 The system database shall provide the capability to store notification messages.**

**(U) 3.2.18.9 The system database shall provide the capability to store user account information.**

**(U) 3.2.18.10 The system database shall provide the capability to store user preferences.**

**(U) 3.2.18.11 The system database shall provide the capability to store list of value (lookup) types of data for use across the application to ensure consistency.**

**(U) 3.2.18.12 The system database shall provide the capability to store canned searches for use by all system users.**

**(U) 3.2.18.13 The system database shall provide the capability to store user-defined searches for later use by the user.**

(U) This use includes recall and modification.

**(U) 3.2.18.14 The system database shall provide the capability to store a defined workflow.**

(U) This includes all of its associated steps, nodes, rules and status information as appropriate.

**(U) 3.2.18.15 The system database shall provide the capability to store the user work queue data.**

(U) This includes data associated with a user and a workflow.

**(U) 3.2.18.16 The system database shall provide the capability to store the group work queue data.**

(U) This includes data associated with a user and a workflow.

**(U) 3.2.18.17 The system database shall provide the capability to store simulation data.**

(U) This includes pre-canned, artificial messages for use in exercises and for testing purposes.

**(U) 3.2.18.18 The system database shall provide the capability to store group account information.**

**(U) 3.2.18.19 The system database shall provide the capability to store product templates.**

**(U) 3.2.18.20 The system database shall provide the capability to store site-level system configuration information.**

**(U) 3.2.18.21 The system database shall provide the capability to store copies of all information transmitted to external systems.**

(U) This includes transmitted data whether successful or unsuccessful.

**(U) 3.2.18.22 The system database shall provide for online access to all stored data information, through the application, for a minimum of five years.**

(U) This includes audit and transmitted data.

**(U) 3.2.18.23 The system database shall associate stored data to the user who performed CRUDA operations on it.**

(U) These operations are create, read, update, delete, archive (CRUDA).

**(U) 3.2.18.24 The system database shall store widget settings for each user preference (i.e. URL, size, shape, workspace, customization, dashboard configuration) .**

### (U) Installation and Configuration

(U) The following subsection describes the system requirements for installation and configuration.

**(U) 3.2.19.1 The system shall be developed such that it can be built with a single command.**

(U) For example, an *ant* or *maven* target.

**(U) 3.2.19.2 The system shall be installable with simple scripts.**

**(U) 3.2.19.3 The system shall provide test scripts to ensure the system is installed correctly.**

(U) These test scripts should also test that the system is deployed correctly.

**(U) 3.2.19.4 The system shall allow the configuration of key system settings without requiring a software release.**

**(U) 3.2.19.5 The system shall provide the ability to specify server connection information in a configuration file.**

**(U)3.2.19.6 The system shall support the use of scripts to create required database artifacts.**

**(U) 3.2.19.7 The system shall support the use of scripts to load initialization data into the database.**

(U) This includes what is also known as *seed* data.

**(U) 3.2.19.8 The install process shall be documented.**

(U) Provide both hardcopy and softcopy install process documentation with the system.

**(U) 3.2.19.9 The system shall provide a capability for its initialization.**

**(U) 3.2.19.10 The system shall provide the capability for an orderly controlled shutdown of operations.**

**(U) 3.2.19.11 The system shall provide the capability to update configuration setting for selected server-side functionality.**

(U) For example, email server.

**(U) 3.2.19.12 The system shall be able to perform a backup operation on request.**

(U) Backup operations can be on the entire system, a component, or individual files.

**(U) 3.2.19.13 The system shall be able to perform a restore operation on request.**

(U) Restore operations can be for the entire system, a component, or individual files

**(U) 3.2.19.14 The system shall be able to perform a backup of security-relevant functions on request.**

(U) This includes backing up security-relevant data.

**(U) 3.2.19.15 The system shall be able to restore, on request, the security-relevant functions up to the last backup archive.**

(U) This includes restoring security-relevant data.

**(U) 3.2.19.16 The system shall be capable of being restored to the last known secure configuration through the application of the recorded changes to security-relevant functions.**

(U) This includes security-relevant data.

### (U) Help

(U) The following subsection describes the system requirements for help. Control all data this service stores and accesses by security labeling to support Mandatory Access Control requirements.

**(U) 3.2.20.1 The system shall provide an online help capability.**

**(U) 3.2.20.2 The system shall provide the capability for privileged users to access contact information.**

(U) This includes saving and loading technical and operational points of contact for information and assistance.

**(U) 3.2.20.3 The system shall provide on-line documentation.**

(U) This documentation includes the following.

* User Guide
* System Administrator Guide
* References

**(U) 3.2.20.4 The system shall provide the capability for on-line problem reporting.**

### (U) Deployment

(U) The following subsection describes the system requirements for deployment.

**(U) 3.2.21.1 The system shall be capable of being deployed in a high assurance (HA) deployment configuration.**

**(U) 3.2.21.2 The system shall be capable of supporting Elastic Load Balancing (ELB).**

**(U) 3.2.21.3 The system shall be able to support application auto-scaling.**

**(U) 3.2.21.4 The system data capability shall be able to support elastic block storage volumes.**

(U) This includes a system database and/or data store.

## (U) SWIF Application Requirements

### (U/FOUO) Planning Application

(**U/FOUO**) The following subsection describes the system requirements for the Planning application. The Planning application gives users the ability to generate Plans and Concept of Operations (CONOPS) work products, as well as facilitate planning within the Joint Planning process. Use security labeling to support Mandatory Access Control requirements to control all data this service stores and accesses.

**(U//FOUO) 3.3.1.1 The system shall include a Planning application.**

**(U//FOUO) 3.3.1.2 The system Planning application shall operate within the SWIF architecture.**

**(U//FOUO) 3.3.1.3 The system Planning application shall use the SWIF Common Services.**

(U) This includes interacting with the common services.

**(U//FOUO) 3.3.1.4 The system Planning application shall be capable of using the widgets within the SWIF Core Services.**

**(U//FOUO) 3.3.1.5 The system shall include Planning widgets that allow users to perform CRUDA operations on Plans.**

(U) These operations are create, read, update, delete, archive (CRUDA).

**(U//FOUO) 3.3.1.6 The system shall include Concept of Operations (CONOPS) widgets that allow users to perform CRUDA operations on CONOPS.**

(U) These operations are create, read, update, delete, archive (CRUDA).

**(U//FOUO) 3.3.1.7 The system Planning application shall be capable of using the System and Common Services within the SWIF Common Services.**

**(U//FOUO) 3.3.1.8 The system Planning Services shall be capable of using the Visualization Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.9 The system Planning application shall be capable of using the User Account Management (UAM) Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.10 The system Planning application shall be capable of using the Groups Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.11 The system Planning application shall be capable of using the Search Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.12 The system Planning application shall be capable of using the Workflow and Queues Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.13 The system Planning application shall be capable of using the Import Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.14 The system Planning application shall be capable of using the Export Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.15 The system Planning application shall be capable of using the Named Area of Interest (NAI) Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.16 The system Planning application shall be capable of using the Analytic Tools within the SWIF Common Services.**

**(U//FOUO) 3.3.1.17 The system Planning application shall be capable of using the Production Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.18 The system Planning application shall be capable of using the Notification Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.19 The system Planning application shall be capable of using the Subscription Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.20 The system Planning application shall be capable of using the Audit Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.21 The system Planning application shall be capable of using the Usage and Performance Analytic Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.22 The system Planning application shall be capable of using the System Configuration Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.23 The system Planning application shall be capable of using the User Preference Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.24 The system Planning application shall be capable of storing data in the system’s database.**

**(U//FOUO) 3.3.1.25 The system Planning application shall comply with the UI requirements described within this document to provide a consistent user experience.**

**(U//FOUO) 3.3.1.26 The system Planning application shall be capable of using the Help Service within the SWIF Common Services.**

**(U//FOUO) 3.3.1.27 The system Planning Services shall provide the capability for a user to** **perform CRUDA operations on Plans.**

(U) These operations are create, read, update, delete, archive (CRUDA).

**(U//FOUO) 3.3.1.28 The system Planning Services shall provide the capability for a user to perform CRUDA operations on Concepts of Operations (CONOPS).**

(U) These operations are create, read, update, delete, archive (CRUDA).

**(U//FOUO) 3.3.1.29 The system Planning Services shall provide the capability for a user to perform CRUDA operations on Capabilities.**

(U) These operations are create, read, update, delete, archive (CRUDA).

**(U//FOUO) 3.3.1.30 The system shall provide the capability for a user to set discretionary access (users or groups) to the Planning Services.**

**(U//FOUO) 3.3.1.31 The system shall provide the capability for a user to develop a Concept of Operations (CONOP) for the selected capability specific to a Plan.**

**(U//FOUO) 3.3.1.32 The system shall provide the capability for a user to display nodes and relationships****.**

**(U//FOUO) 3.3.1.33 The system shall provide the capability for a user to create a user-defined diagram of the overall Plan.**

**(U//FOUO) 3.3.1.34 The system shall provide the capability for a user to create a product from a Plan.**

(U) This includes creating a product from a Concept of Operations (CONOPS).

**(U//FOUO) 3.3.1.35 The system shall provide the capability for a user to associate Capabilities to a Plan.**

**(U//FOUO) 3.3.1.36 The system shall provide the capability for a user to associate Target Folders to a Plan.**

**(U//FOUO) 3.3.1.37 The system shall provide the capability for a user to associate Target Folders and Capabilities to each other in support of creating a decision matrix****.**

**(U//FOUO) 3.3.1.38 The system shall provide the capability for a user to associate Plans to Concepts of Operations (CONOPS).**

**(U//FOUO) 3.3.1.39 The system shall provide the capability for a user to create a user-defined capability of a specific Plan.**

**(U//FOUO) 3.3.1.40 The system shall provide the capability for a user to create a SWIF Common Datta Model (CDM) Record.**

**(U//FOUO) 3.3.1.41 The system shall provide the ability to link all created objects to a unique identifier associated with the SWIF user’s products.**

These include Plans, CONOPS and Capabilities.

**(U//FOUO) 3.3.1.42 The system shall provide the capability for a user to mark created items with the appropriate security markings.**

(U) These markings include classification and any other security control markings.

**(U//FOUO) 3.3.1.43 The system shall provide the capability for a user to set discretionary access on previously created items.**

(U) This includes users or groups and Plans, CONOPS and Capabilities.

**(U//FOUO) 3.3.1.44 The system shall provide the capability for a user to import Capabilities from an external source.**

**(U//FOUO) 3.3.1.45 The system shall provide the capability for a user to import Target Folders from an external source.**

**(U//FOUO) 3.3.1.46 The system shall provide the capability for a user to import other data for subsequent Planning analysis.**

**(U//FOUO) 3.3.1.47 The system shall provide problem definition tools.**

(U) These tools include graphic organizers, conceptual models, mind maps, and causal loop diagrams.

**(U//FOUO) 3.3.1.48 The system shall provide decision support tools.**

(U) These tools include synthesis, ranking, trade-off analysis, multi-criteria decision, and shared vision model tools.

**(U//FOUO) 3.3.1.49 The system shall provide a course of action (COA) development support capability.**

**(U//FOUO) 3.3.1.50 The system shall provide a simulation capability to assist in course of action (COA) development.**

### (U) Target Folder Application

(U) The following subsection describes the system requirements for the Target Folder application. Use security labeling to support Mandatory Access Control requirements to control all data this service stores and accesses.

**(U) 3.3.2.1 The system shall include a Target Folder application.**

**(U) 3.3.2.2 The Target Folder application shall work with the SWIF core services.**

**(U) 3.3.2.3 The system shall include a Target Folder widget that allows users to perform CRUDA operations on targets.**

(U) These operations are create, read, update, delete, archive (CRUDA).

**(U) 3.3.2.4 The system shall provide the capability for the user to perform target feasibility analysis.**

## (U) System Interface Requirements

### (U) Interface Identification and Diagrams



*[Figure is* ***U//FOUO****]*

1. Figure : (U) SWIF External Interfaces

### (U) Internal Interfaces

(U) The following subsection describes the system requirements for internal interfaces.

**(U) 3.4.2.1 The system’s hardware interfaces shall be compliant with referenced operations and computer/communications security requirements and standards.**

**(U) 3.4.2.2 The system shall be capable of operating on Ethernet-based networks that support protocols including TCP/IP and HTTPS.**

**(U) 3.4.2.3.The system shall provide the capability to interface with a database.**

**(U) 3.4.2.4 The system shall provide for secure connections (TLS) for all thick client communication.**

### (U) External Interfaces

(U) The following subsection describes the system requirements for the SWIF interfaces to external systems. The SWIF Interface Control Document (ICD; not yet produced) contains a description of the each interface including data formats, communications protocols, and information assurance.

**(U) 3.4.3.1 The configuration of the system’s controlled interface to the external systems shall be restricted to privileged Site Administrators.**

**(U) 3.4.3.2 Data transmitted from an external systems controlled interface shall be audited.**

**(U) 3.4.3.3 Data sent from external systems to the SWIF system shall include a classification marking for the classification of the content of the data exchange.**

**(U) 3.4.3.4 The system shall provide for secure network connections (HTTPS) for all Web interfaces.**

(U) This requirement includes Web service methods.

**(U) 3.4.3.5 The system shall provide the capability to interface with an external email server.**

(U) This requirement applies if configured to do so in the host environment.

**(U) 3.4.3.6 The system shall provide a Web interface for all actions initiated by users.**

**(U) 3.4.3.7 The system shall provide for a controlled interface with an image library.**

**(U) 3.4.3.8 The system shall provide an OpenSearch interface to allow external systems to access SWIF data holdings.**

(U) This interface includes subscribing to SWIF data holdings.

**(U) 3.4.3.9 The system shall provide a Web Processing Service (WPS) interface to allow external systems to access SWIF data holdings.**

(U) This interface includes subscribing to SWIF data holdings.

**(U) 3.4.3.10 The system shall provide a controlled interface with WMS/WFS-enabled servers.**

**(U) 3.4.3.11 The system shall provide for a controlled interface with a map server.**

**(U) 3.4.3.12 The system shall provide a capability for managing taskings to external systems.**

**(U) 3.4.3.13 The system shall provide a controlled interface with requirements management systems.**

**(U) 3.4.3.14 The system shall provide a controlled interface with external analytic systems.**

**(U) 3.4.3.15 The system shall provide the capability to monitor communications between the SWIF system and external systems.**

**(U) 3.4.3.16 The system shall provide a controlled interface with the Modernized Integrated Data Bases (MIDB).**

**(U) 3.4.3.17 The system shall provide the capability to export SWIF documents into a SWIF-defined format.**

## (U) System Internal Data Requirements

(U) The SWIF System/Subsystem Specification is a system-level document and does not define the internal details of the SWIF subsystems and their functions or the internal data structures for each subsystem. The data structures will be documented in the SWIF Logical Data Model (LDM).

## (U) Adaptation Requirements

(U) The following subsection describes the system adaptation requirements.

**(U) 3.6.1 A test/training system shall be made available.**

**(U) 3.6.2 The test/training system shall have, as a minimum, the same functionality as the operational system.**

**(U) 3.6.3 A variant of the system shall be made available to support a Coalition environment.**

## (U) Safety Requirements

(U) The following subsection describes the system safety requirements.

**(U) 3.7.1** **The system shall comply with best safety practices to minimize potential hazards.**

(U) This requirement is to minimize hazards to personnel, property, and the environment (e.g., OSHA, electrical, and fire safety, and the restriction on the use of dangerous materials).

**(U) 3.7.2 Warnings shall be issued to users before system shutdown.**

## (U) Security and Privacy Requirements

(U) The requirements in this specification assume the system will be hosted on platforms that are protected at an appropriate level for the information processed on it. These protections include appropriate levels of physical, personnel, communications, emanations, and technical surveillance countermeasures (TSCM) security, as required in Intelligence Community Directives (ICDs). The system will be certified and accredited in accordance with the target network accreditor.

(U) The full scope of security requirements for the SWIF system is detailed in the SWIF Certification and Accreditation documentation.

### (U) Security

(U) The following requirements describe the system’s requirements for security.

**(U) 3.8.1.1 The system shall comply with Intelligence Community Directives on security controls on the dissemination of intelligence information.**

(U) Note: Intelligence Community Directive 710, *Classification and Control Markings System*, has replaced sections I-IV and XI-XVI of DCID 6/6, *Security Controls on the Dissemination of Intelligence Information* (sections V-X and Annexes A and B of DCID 6/6 remain in effect until otherwise rescinded). Pay particular attention to the portions of these directives that pertain to Executive Order 12958 as it pertains to marking classified information.

**(U) 3.8.1.2 The system shall meet collateral Department of Defense security certification and accreditation requirements.**

**(U) 3.8.1.3 The system shall meet Intelligence Community Sensitive Compartmented Information (SCI) security certification/accreditation requirements, as applicable.**

**(U) 3.8.1.4 The system shall be accessible only to authorized users.**

**(U) 3.8.1.5 The system shall require a user to log on to the system before the user can access the system application and its resources for any functionality.**

**(U) 3.8.1.6 The system shall allow for a visitor account.**

(U) This guest or visitor account will be treated as a user with *Unclassified* security clearance.

**(U) 3.8.1.7 The system shall allow for only a single session per user account.**

(U) If a user has an active session and tries to log in using a different client machine or browser; the prior session will be invalidated

**(U) 3.8.1.8 The system shall include an Identification and Authentication (I&A) management mechanism that uniquely identifies and authenticates.**

(U) This mechanism also associates the user identifier with all auditable actions taken by that user.

**(U) 3.8.1.9 The system shall provide for secure user login authentication and authorization for system access.**

**(U) 3.8.1.10 The system shall include read-only classification banners within each user interface (UI) screen displayed.**

**(U) 3.8.1.11 The system shall display classification banners within each system window being displayed with a background color matching the appropriate classification level.**

**(U) 3.8.1.12 The system shall allow the Site Administrator to set the classification instructions in the banner displayed to the system user.** **(unclear if available)**

**(U) 3.8.1.13 All factory (including commercial) default passwords for the system shall be changed before operational deployment.**

**(U) 3.8.1.14 The system shall ensure system notifications are destined for the correct recipient, based on the type of notification.**

**(U) 3.8.1.15** **The system shall ensure the content of a notification for the intended recipient is appropriate for the type of notification.**

**(U) 3.8.1.16 The system shall validate the integrity information associated with each notification.**

(U) Integrity information includes integrity seal, or non-repudiation data.

**(U) 3.8.1.17 The system shall provide the ability to monitor notifications transmitted from the system to external systems.**

(U) Included in the monitoring function is and a record capability.

**(U) 3.8.1.18 The system shall provide a role-based access control system to support a single log-on capability based on an individual user profile.**

(U) This process consists of strong identification and authorization and formal accesses (clearances).

**(U) 3.8.1.19 The system shall authenticate each user using strong authentication mechanisms over secure channels before authorizing access to the system.**

**(U) 3.8.1.20 The system shall only use Transport Layer Security (TLS) encryption mechanisms that are Federal Information Processing Standards (FIPS) 140-2 compliant.**

(U) Note: the system cannot control the encryption modules and methods used on the network.

**(U) 3.8.1.21 The system shall protect all identified data items.**

This protection will be by row or attribute based security settings.

**(U) 3.8.1.22 The system shall restrict read access to data based on Controlled Access Program Coordination Office (CAPCO) guidelines (including classification).**

**(U) 3.8.1.23 The system shall restrict access to actions based on roles with associated privileges.**

**(U) 3.8.1.24 The system shall support the ability of a user to be able to hide his account from appearing in objects associated with system.**

(**U//FOUO**) This includes group lists or other objects such as Plans, CONOPS, etc.

**(U) 3.8.1.25 The system shall support the ability of a user to be able to associate an alias with the user’s account.**

(**U//FOUO**) The alias name would appear in lieu of the user’s name or contact information in group lists or if associated with objects in the system (e.g., Plans, CONOPS, etc.)

**(U) 3.8.1.26 The system shall be able to associate external user authentication information to a SWIF Role.**

(U) This includes DCADS or external LDAP server information.

**(U) 3.8.1.27 The system shall enforce password complexity in compliance with the targeted deployment network.**

**(U) 3.8.1.28 The system shall establish a trusted path to each user.**

(U) Once the system establishes a trusted path it will then identify and authenticate each user.

**(U) 3.8.1.29 Upon successful identification and authentication, the system shall establish a protected path between each authorized user and the system.**

(U) This protected path will provide the following characteristics:

* Protect confidentiality of data during transmission between the authorized user and the system.
* Protect integrity of data during transmission between the authorized user and the system.
* Provide a distinct communication channel between each authorized user and the system.

**(U) 3.8.1.30 The system shall provide a mechanism that will prevent unauthorized use of security-relevant system functions including related data.**

**(U) 3.8.1.31 The system shall provide a mechanism that will detect unauthorized use of security-relevant system functions including related data.**

**(U) 3.8.1.32 The system shall generate an audit record for unauthorized attempts to use security-relevant functions including related data.**

**(U) 3.8.1.33 The system shall provide a mechanism that will prevent the unauthorized modification of security-relevant functions including related data.**

**(U) 3.8.1.34 The system shall provide a mechanism to detect unauthorized modification of security-relevant functions including related data.**

**(U) 3.8.1.35 The system shall generate an audit record for unauthorized attempts to modify security-relevant functions including related data.**

**(U) 3.8.1.36 The system shall provide a mechanism that will enforce the “Principle of Least Privilege” on security-relevant functions.**

**(U) 3.8.1.37 The system shall prevent interference with its operation by removing all residual data generated during its processing when that processing is concluded.**

**(U) 3.8.1.38 The system shall prevent access to information previously contained in objects that have been unallocated.**

(U) Unallocated objects may be subsequently reallocated.

**(U) 3.8.1.39 The system shall provide a mechanism that will prevent the bypass of security functions.**

**(U) 3.8.1.40 The system shall provide a mechanism to search specified objects for malicious content defined by the malicious content profile(s).**

**(U) 3.8.1.41 If malicious content is found, the system shall generate an audit record and perform other actions specified by the requestor.**

**(U) 3.8.1.42 The audit record for the malicious content detection shall support evaluating the detected content.**

(U) This includes the identity requesting the search, the identity of the object, and the identity of the malicious content.

**(U) 3.8.1.43 The system shall assign restrictive default values for the access control attributes of all subjects and objects when they are created.**

(U) For components supporting a MAC policy, the system shall assign the MAC attributes to the access control attributes for all subjects and objects as they are created. For components supporting a DAC policy, the system shall assign the DAC attributes to the access control attributes for all subjects and objects as they are created.

**(U) 3.8.1.44 The system shall assign the MAC attributes to the access control attributes for all subjects and objects residing on systems enforcing a MAC policy.**

**(U) 3.8.1.45 The system shall provide the capability for a subject to obtain the DAC attributes (e.g., group membership or access type) for a particular subject (user) or object they dominate.**

**(U) 3.8.1.46 The system shall provide the ability for a subject residing on systems enforcing a MAC policy to obtain the MAC attribute values of a subject or object they dominate.**

**(U) 3.8.1.47 The system shall provide the ability for a subject to determine whether it has DAC access to a named object.**

**(U) 3.8.1.48 The system shall be able to compare two sets of MAC attribute values to determine their dominance relationship.**

**(U) 3.8.1.49 The system shall be able to determine whether the values for the MAC attributes assigned to a subject or object are valid, to include conforming to the relationship rules for MAC attributes.**

**(U) 3.8.1.50 The system shall mediate access to an object by a subject, based on the access control attributes and policies extant on a given component.**

**(U) 3.8.1.51 The system shall provide a service to generate non-repudiation data.**

(U) This non-repudiation data generated shall contain at least the following:

* identity of the requesting user,
* date and time of the request,
* identity of the data, and
* a unique identifier for the data (e.g., a strong hash) for which the requestor is claiming responsibility, bound together by a cryptographic seal.

**(U) 3.8.1.53 The system shall generate a non-repudiation record whenever the system generates non-repudiation data.**

**(U) 3.8.1.54 The system shall provide a service to verify the authenticity of non-repudiation data.**

**(U) 3.8.1.55 The system shall generate a non-repudiation record whenever the system validates non-repudiation data.**

**(U) 3.8.1.56 The system shall generate a non-repudiation record when the system verifies the authenticity of non-repudiation data.**

(U) A non-repudiation record shall contain at least the following:

* The type of non-repudiation action taken (i.e., generation, verification);
* The date and time of the action;
* The result of the action;
* The identity of the object; and,
* The non-repudiation data bound to the object.

**(U) 3.8.1.57 The system shall provide the capability for the ISSO to retrieve non-repudiation records.**

(U) Retrieval criteria can include date/time the non-repudiation record was generated, identity of the user responsible for non-repudiation action, identity of the object referenced by the non-repudiation data).

**(U) 3.8.1.58 The system shall preserve non-repudiation records for forensic analysis.**

**(U) 3.8.1.59 The system shall generate audit records capturing security-relevant events.**

(U) All audit records shall include the following:

* The type of event (e.g., data authentication)
* The date and time of the event
* The result of the action
* The identity of the entity performing the action
* Any event-specific data

**(U) 3.8.1.60 The system shall store generated audit events into an audit log that is protected against unauthorized modification.**

**(U) 3.8.1.61 The audit log shall be capable of being exported by authorized privileged users.**

(U) This includes the ability of an authorized privileged user to print the audit log.

**(U) 3.8.1.62 The system shall provide the capability for the ISSO to obtain an audit record.**

(U) The ISSO can use specific criteria (e.g., time range, user ID, object ID, subsystem).

**(U) 3.8.1.63 The system shall be able to perform a backup operation.**

(U) This backup operation can be on the entire system, a component, or individual files on request.

**(U) 3.8.1.64 The system shall be able to perform a restore operation.**

(U) This backup operation can be on the entire system, a component, or individual files on request.

**(U) 3.8.1.65 The system shall be able to perform a backup of security-relevant functions including data on request.**

**(U) 3.8.1.66 The system shall be able to restore, on request, the security-relevant functions including data up to the last backup archive.**

**(U) 3.8.1.67 The systems shall be capable of being restored to the last known secure configuration through the application of the recorded changes to security-relevant data including functions.**

**(U) 3.8.1.68 The system shall provide the capability to generate an integrity seal for data that permits modification of the original data to be detected.**

**(U) 3.8.1.69 The system shall provide the capability to validate the integrity seal that has been generated for data.**

**(U) 3.8.1.70 The system shall provide the capability to ensure the confidentiality of data through encryption.**

**(U) 3.8.1.71 The system shall provide the capability to decrypt encrypted data.**

**(U) 3.8.1.72 The system shall require all users interacting with the system to identify themselves to include authenticating their claimed identity.**

(U) If the user employs a direct connection to the system (i.e., using a device attached to a system component by a private, physically or logically isolated link), the user may use reusable passwords (conforming to the SWIF password policy). If the user employs a shared or remote connection to the system (i.e., using a device attached to a network or broadcast media), the user must use a single-use authenticator or a cryptographic authentication mechanism (i.e., shall employ strong user identification and authentication).

**(U) 3.8.1.73 The system shall notify users that their authenticator will expire within an ISSO-specified period prior to the authenticator’s expiration.**

**(U) 3.8.1.74 The system shall make an authenticator unusable after an ISSO-specified lifetime.**

**(U) 3.8.1.75 The system shall be able to obtain identification and authentication attributes (e.g., user ID) for a user from the user profile identification and authentication attributes.**

**(U) 3.8.1.76 The system shall invoke the appropriate user interface based on user authentication.**

(U) This occurs after General and Privileged Users have successfully identified and authenticated themselves and have selected a role.

**(U) 3.8.1.77 The system shall provide the capability for an individual authorized user to update the user’s own user identification and authentication attributes maintained in the user profile.**

(U) Additionally, an ISSO can update any user’s identification and authentication attributes maintained in the user’s profile.

**(U) 3.8.1.78 The system shall ensure that user passwords are sufficiently strong for reliable authentication by conforming with FIPS 181, Automated Password Generator (APG), October 1993.**

**(U) 3.8.1.79 The system shall provide a reliable time source to its components.**

(U) The reliable time source supports the generation of non-repudiation and audit data and subsequent analysis of merged audit data across all system components.

**(U) 3.8.1.80 The system shall provide the capability to adjust the reliable time source with values obtained from an authorized reference time source.**

(U) The ISSO or Administrator is the privileged user able to initialize or update the system time source.

### (U) Privacy

(U) The following requirements describe the system’s requirements for privacy.

**(U) 3.8.2.1 The system shall comply with the provisions of the Foreign Intelligence Surveillance Act as it pertains to the collection and retention of data on U.S. persons.**

**(U) 3.8.2.2 The system shall provide the capability to notify the Site Administrator automatically when information held about a U.S. Person is reaching its expiration date.**

(U) This notification is so that the Administrator can expunge or extend the expiration date per compliance with the law.

**(U) 3.8.2.3 The system shall comply with the Privacy Act of 1974.**

(U) This act governs the collection, maintenance, use, and dissemination of personally identifiable information about users of the system.

## (U) System Environment Requirements

(U) The following subsection describes the environment in which the system must operate. The physical facility, organizational policies and procedures, personnel, or the organization’s IT infrastructure must meet the system’s IT environment requirements.

(U) Assumptions include the following:

* The system will operate in a secure facility approved to process data classified at the Top Secret/SCI level.
* The organizational policies and procedures will meet the applicable requirements for the system.
* Interactions with SWIF from external systems will be controlled.
* Interactions with SWIF from the organization’s internal network will be controlled.
* In general, SWIF expects that the general infrastructure for the organization will deny all data flows to it, except IP data packets addressed to ports explicitly authorized for SWIF operation.

**(U) 3.9.1 The system shall operate in a commercial computer environment using commercial electrical power.**

**(U) 3.9.2 The system shall not impose any environmental constraints on the host hardware system.**

## (U) Computer Resource Requirements

### (U) Computer Hardware Requirements

(U) The following subsection describes the system computer hardware requirements.

**(U) 3.10.1.1 The system shall be capable of having the servers deployed on different host machines.**

(U) The system servers include the application and the database servers.

**(U) 3.10.1.2 If deployed on multiple host machines, the system shall be deployed on a server which meets the current system capabilities.**

Current system minimum capabilities follow:

* 4 Gigabyte RAM
* 1 Terabyte hard drive
* 2 x dual-core processors
* Linux, OS X, WinOS operating system

**(U) 3.10.1.3 The system shall be capable of being deployed with the servers on the same host machine.**

(U) The system servers include the application and the database servers.

**(U) 3.10.1.4 If deployed on a single host machine, the system shall be deployed on a server which meets the current system minimum capabilities.**

(U) Current system minimum capabilities follow:

* 4 Gigabyte RAM
* 1 Terabyte hard drive
* 2 x dual-core processors
* Linux, OS X, WinOS operating system

### (U) Computer Hardware Resource Utilization Requirements

(U) The following is the maximum hardware resource utilization requirements for SWIF.

[Note: Need SWIF Team input in this area. This includes maximum allowable use of processor capacity, memory capacity, I/O device capacity, auxiliary storage device capacity, and comms/network equipment capacity. The requirements can be stated as percentages of capacity of each computer hardware resource include condition under which the resource utilization is to be measured.]

### (U) Computer Software Requirements

(U) The following subparagraph describes the system computer software requirements.

**(U) 3.10.3.1 The system shall operate, as a minimum, on two servers.**

(U) The current minimum system application and the database servers are the following.

* Tomcat Web Application or Servlet Server
* Mongo Database Server

**(U) 3.10.3.2 The system server shall support cross-platform deployment.**

(U) Cross-platform deployment includes, for example, deployment on a WinOS or Linux-based operating system in addition to OS-X.

* OS X Requirements:
* OS X Version 10.6 (Snow Leopard)
* Windows Operating System Requirements:
* Windows 7
* Windows Server 2003/2008/2012
* Linux Requirements
* Red Hat Enterprise Linux (RHEL)
* Community Enterprise Operating System (CENTOS)
* Secure Linux (SELinux)
* Fedora

**(U) 3.10.3.3 The system shall support multiple browsers.**

(U) The system currently supports the following browsers:

* Safari
* Chrome
* Firefox

**(U) 3.10.3.4 The system shall deny access by users who attempt to access the system using a Web browser that has not been approved by the target network Chief Information Officer (CIO).**

### (U) Computer Communications Requirements

(U) SWIF will use the existing organization’s facilities to communicate with external systems. The objective SWIF system must comply with the communications requirements of its external interface, which involve hardware media and connections. There are no other computer communications requirements levied on SWIF. With the exception of the requirements below, SWIF does not directly levy any computer communications requirements on its external environment (i.e., the organization’s infrastructure).

**(U) 3.10.4.1 In accordance with the hosting network, the system shall use mechanisms to prevent the hijacking of a communications session.**

(U) Protect communications links, data communications and networks with COMSEC policies appropriate for the sensitivity level of the channel. Mechanisms to detect and prevent the hijacking of a communications session include encrypted communications channels.

**(U) 3.10.4.2 In accordance with the hosting network, the system shall use Special Purpose Network systems with associated networks accredited to handle classified information.**

(U) Network latencies will affect the overall user-experienced transaction response times. Currently, there are no quality of service (QOS) or service level agreements (SLA) supported by the hosted network for carrying the SWIF system transactions. Therefore, the actual latency incurred as a result of the target network will not be counted as part of the overall response times for the external transaction.

(U) Assuming the minimum hardware requirements are met, the following are data transmission and responsiveness requirements.

**(U) 3.10.4.3 The system’s latency shall not exceed 5 seconds to respond to a service request.**

(U) This does not include external network latency outside the control of the SWIF system.

**(U) 3.10.4.4 The system shall support data ingest of at least 1000 messages in an hour.**

(U) This is assuming 100 KB per message.

**(U) 3.10.4.5 The system shall support 50 concurrent users per site installation.**

**(U) 3.10.4.6 The system shall provide error messages for failed transmissions.**

**(U) 3.10.4.7 The systems shall provide the capability to generate and display metrics.**

(U) This includes metrics on the following:

* Usage
* Performance

## (U) System Quality Factors

### (U) Functionality

(U) Functional requirements are specified in Sections 3.2 and 3.3.

### (U) Performance

(U) The following subsection describes the system performance requirements.

**(U) 3.11.2.1 The average response time for a system transaction must not exceed five (5) seconds.**

**(U) 3.11.2.2 The maximum response time for a system transaction must not exceed ten (10) seconds.**

**(U) 3.11.2.3 The system must be capable of handling X transactions per second during normal operations.**

**(U) 3.11.2.4 The system must be capable of handling X transactions per second during emergency operations.**

**(U) 3.11.2.5 The system must be capable of supporting X number of simultaneous users during peacetime mode.**

**(U) 3.11.2.6 The system must be capable of supporting X number of simultaneous users during wartime mode.**

**(U) 3.11.2.7 The system must be capable of operating in a degraded mode.**

**(U) 3.11.2.8 Resource utilization (memory, disk, communications).**

**(U) 3.11.2.9 The system must verify user login information within five (5) seconds.**

**(U) 3.11.2.10 Queries must return results within five (5) seconds.**

**(U) 3.11.2.11 System functions must be initiated within 500 μsecs after their selection.**

**(U) 3.11.2.12 User-selected pages must be displayed within five (5) seconds after their selection.**

### (U) Reliability

(U) The following subsection describes the system requirements for reliability.

**(U) 3.11.3.1 Failure of a given system component shall not precipitate a failure in its backup equipment.**

(U) This includes a site failure and redundant equipment failure.

**(U) 3.11.3.2 Failure of the system’s software components shall not cause failures in interfacing components.**

(U) This includes failure of one or more system components; such a failure will not cause failures in interfacing software segments or host hardware components.

**(U) 3.11.3.3 The system shall achieve a mean time between critical failures (MTBCF) of at least 5,000 hours.**

(U) MTBCF is defined as the system up-time divided by the number of critical failures. Critical failures are those failures that cause the system to degrade to the point where the mission cannot be accomplished (and may include, but not be limited to, the following causes: any hardware or software failure; design, manufacturing or workmanship defects; physical or functional deterioration; or any other unexplained failure). For purposes of computing MTBCF, failure attributed to the following causes are not considered critical failures: failures compensated by system redundancy (automatically or manually) providing for restoration of operations within thirty minutes; improper installation; misuse, mishandling, or improper operation of equipment. The system MTBCF shall be predicted in accordance with MIL-HDBK-217F or commercially-available empirical data based on operational usage of essentially similar equipment. Ground benign environmental conditions shall apply.

### (U) Maintainability

(U) The following subsection describes the system requirements for maintainability.

Table . (U) STR Priority Descriptions

*[Table is Unclassified]*

| **STR PRIORITY** | **APPLIES IF A PROBLEM COULD HAVE THE FOLLOWING RESULT:** |
| --- | --- |
| 1 | Prevent the accomplishment of an operational or mission essential capability. |
| 2 | a. Adversely affect the accomplishment of an operational or mission essential capability and no work-around solution is known.  b. Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, and no work-around solution is known. |
| 3 | a. Adversely affect the accomplishment of an operational or mission essential capability but a work-around solution is known.  b. Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, but a work-around solution is known. |
| 4 | a. Result in user/operator inconvenience or annoyance but does not affect a required operational or mission essential capability.  b. Result in inconvenience or annoyance, but does not prevent accomplishment of responsibilities. |
| 5 | Result in any other effect. |

**(U) 3.11.4.1 The system shall** **have a Mean Corrective Maintenance Time (MCMT) of no greater than one hour and a Mean Maximum Corrective Time (MMCT) of 2 hours (90th percentile).**

(U) NOTE: Assume maintenance person on-site with all required tools, test equipment, and spares. Corrective maintenance time is defined as the time between system down and system restored to operational status. The MMCT of the hardware shall be predicted in accordance with MIL-HDBK-472, method 2 or 3.

**(U) 3.11.4.2 The system shall mark audit table entries with severity (level) values to assist in isolating defects for their cause.**

(U) Markings can include INFO (Informational), WARN (Warning) and FAIL (Failure).

**(U) 3.11.4.3 To reduce the mean time to repair, the system shall minimize the use of “hard-coding” values.**

(U) Instead, maximize the use of configuration parameters that can be modified while the system is online.

**(U) 3.11.4.4 The system shall be developed in the Java software language to improve maintainability.**

**(U) 3.11.4.5 The system shall be implemented in a layered architecture.**

**(U) 3.11.4.6 The system shall be implemented to be modular.**

**(U)** **3.11.4.7 The system shall be implemented to maximize encapsulation to hide the values or state of a structured data object inside a class, preventing unauthorized parties direct access to them.**

**(U)** **3.11.4.8 The system shall be implemented with well-defined interfaces.**

**(U)** **3.11.4.9 The system shall be implemented using object-orientation and component-based development.**

**(U)** **3.11.4.11 The system design shall be documented in the form of Software Design Descriptions for each component.**

**(U)** **3.11.4.12 The system’s interface design shall be documented in the form of Interface Design Descriptions for each interface defined by the system for use by external systems.**

**(U)** **3.11.4.13 The system’s interface design shall be documented in the form of an Interface Control Document for all of the system’s interfaces.**

**(U)** **3.11.4.14 The system’s software code shall contain comments by the developer to support maintainability.**

**(U)** **3.11.4.15 The system shall be designed and implemented with adherence to project conventions.**

(U) Programming standards and guidelines will be defined and enforced.

**(U)** **3.11.4.16 The average person-time required to fix a Priority 3 defect shall not exceed two person-days.**

This includes regression testing and documentation updating.

**(U)** **3.11.4.17 The average person-time required to fix a Priority 2 defect shall not exceed one person-week.**

(U) This includes regression testing and documentation updating.

**(U)** **3.11.4.18 The average person-time required to make a minor enhancement shall not exceed one person-week.**

(U) This includes testing and documentation updating.

**(U)** **3.11.4.19 Dead code shall not be retained in the system.**

**(U)** **3.11.4.20 Redundant code shall not be retained in the system.**

**(U)** **3.11.4.21 The system shall be designed with enough flexibility to support new protocols as they emerge without requiring a software redesign.**

### (U) Availability

(U) The following requirements describe the system’s requirements for availability. The following failure class definitions are provided for reference. [Note: some requirement statements in this subsection are still under development (as indicated by “X” placeholders.]

Table . (U) Failure Class Definitions

*[Table is Unclassified]*

|  |  |
| --- | --- |
| **Failure Class** | **Definition** |
| Critical | Operations cannot be continued |
| Warning | Operations can be continued, but with reduced capability |
| Information | Operations can be continued |

(U) Availability = MTBF / (MTBF + MTTR). MTTR is the Mean Time To Repair. MTBF is the average time the software is available, whereas the sum of MTBF and MTTR is the average time it should be operational.

(U) Availability in this document is described in terms of the number of nines (e.g., 3 nines = 99.9% and 5 nines = 99.999%). The following table clarifies how rapidly downtime decreases as availability increases.

Table . (U) Availability Description

*[Table is Unclassified]*

|  |  |  |
| --- | --- | --- |
| **Percent Operationally Available** | **Number of Nines** | **Total Downtime Per Year** |
| 90% | 1 | 36 Days 12 Hours |
| 95% | N/A | 18 Days 6 Hours |
| 98% | N/A | 7 Days 7 Hours |
| 99% | 2 | 3 Days 15 Hours |
| 99.9% | 3 | 8 Hours 46 Minutes |
| 99.99% | 4 | 52 Minutes 31 Seconds |
| 99.999% | 5 | 5 Minutes 15 Seconds |
| 99.9999% | 6 | 31.5 Seconds |

**(U)** **3.11.5.1 The MTBF for Critical failures shall be X weeks, averaged over X months.**

**(U)** **3.11.5.2 The minimum time between Critical failures shall be in excess of X days.**

**(U)** **3.11.5.3 The MTBF for Warning failures shall be X weeks, averaged over X months.**

**(U)** **3.11.5.4 The minimum time between Warning failures shall be in excess of X days.**

**(U)** **3.11.5.5 The system shall not have more than five (5) hours of scheduled downtime per month.**

**(U)** **3.11.5.6 The system shall not more than an average of one (1) hour of unscheduled downtime per month.**

**(U)** **3.11.5.7 The MTTR for the system shall not exceed X hours after it has failed.**

**(U)** **3.11.5.8 Administrative reporting shall have an availability of 98%.**

**(U)** **3.11.5.9 All Planning functionality has a planned availability of 24 hours per day, 365 days per year.**

(U) The design goal shall be 99.9% availability.

**(U)** **3.11.5.10 User access to persistent data shall have an availability of 99.999%.**

**(U)** **3.11.5.11 At least one data center shall be available at all times at least 99.999% of the time.**

**(U)** **3.11.5.12 The SWIF system will not provide functionality for capturing memory usage.**

(U) This includes usage for system servers or disk usage. Sites will need to use existing operating tools to capture and display this information, as well as those tools necessary to perform network, database, and system administration beyond those requirements described within this document.

**3.11.5.13 The system shall provide the ability to perform remote maintenance per the host site System Security Authorization Agreement (SSAA)****.**

**3.11.5.14 SWIF availability requirements shall be determined by the** **Project Manager using Information Assurance (IA) Implementation guidance.**

(U) See Intelligence Community Directive (ICD) 503 and DoD Instruction 8500.2, both cited in section 2 of the SWIF SSS.

### (U) Portability

(U) The following requirements describe the system’s requirements for portability.

**(U)****3.11.6.1 The system software shall be capable of being migrated to more powerful processing platforms in support of an expanded user capacity.**

**(U)** **3.11.6.2 The system shall be capable of running on a Linux operating system.**

**(U)** **3.11.6.3 The system shall be capable of running on a Mac operating system.**

**(U)** **3.11.6.4 The system shall be capable of running on a Fedora operating system.**

**(U)** **3.11.6.5 Porting the application from Linux OS to Windows OS shall not require more than 24 person weeks in time.**

(U) Porting includes documentation and testing,

**(U)** **3.11.6.6 The average time needed to port the application to Internet Explorer shall not exceed 12 person weeks.**

(U) Porting includes documentation and testing,

**(U)** **3.11.6.7 The system shall improve portability by isolating operating system calls.**

(U) While it may not be possible to isolate all calls, do so to the maximum extent possible.

**(U)** **3.11.6.8 The system shall minimize the use of machine language.**

**(U)** **3.11.6.9 The system shall be written in Java to maximize portability.**

**(U)** **3.11.6.10 The system shall use open interface standards to maximize portability.**

**(U)** **3.11.6.11 The system shall maximize the use of open interface standards.**

(U) Use open standards such as Enterprise Java Beans for interfaces, distribution, and communications.

### (U) Reusability

(U) The following subsection describes the system requirements for reusability.

**(U)** **3.11.7.1 Reusability shall be considered in the design of SWIF.**

**(U)** **3.11.7.2 The architecture of service components for SWIF shall consider existing APIs.**

(U) Consider Open Standards in addition to existing APIs.

**(U)** **3.11.7.3 A minimum of 30% of the application’s software shall be potentially reusable on future endeavors.**

### (U) Testability

(U) The following subsection describes the system requirements for testability.

**(U)** **3.11.8.1 The system shall be compliant with the requirements specified by the Joint Interoperability Test Command (JITC).**

**(U)** **3.11.8.2 Only testers shall test system software.**

(U) Only users with a Tester role are authorized to use test interfaces and only for SWIF testing purposes.

**(U)** **3.11.8.3 The system shall provide a test interface that enables its state to be observed.**

**(U)** **3.11.8.4 For defined interfaces with external systems, the system shall be delivered with associated test software including test data that is sufficient to enable testing between the system and the external system.**

**(U)** **3.11.8.5 The system shall provide a human interface that enables the user with the Tester role to perform system testing tasks.**

**(U)** **3.11.8.6 The system shall include built-in self-test software that automatically tests the system while it is in operation.**

(U) The built-in self-test software also will work continuously while the system is in operation.

### (U) Usability

(U) The following requirements describe the system’s requirements for usability. Usability for the system includes the following qualities:

* Credibility. The degree to which users are confident with and have trust that the system’s output and behavior are correct and content is authoritative.
* Ease to Entry. The ease with which users can start using the system.
* Ease to Learn. The degree to which representative users can learn to use the system to perform their tasks.
* Ease of Remembering. Either the degree to which occasional users can remember how to use the system to perform common tasks or the degree to which regular users can remember how to use the system to perform infrequent tasks.
* Ease to Use. The ease with which users can use the system to perform their tasks.
* Effectiveness. The degree to which the system enables users to efficiently perform their tasks.
* Error Minimization. The degree to which the system minimizes the number of errors that its users make.
* Navigability. The degree to which users can move through the user interface or documentation to find desired content and to perform their tasks.
* Preference. The degree to which users prefer the system over its alternatives or the way they previously completed their work.
* Retrievability. The ease with which the system enables users to obtain information in a form that is useful to them (e.g., print out a formatted report, make a copy of a work product, etc.).
* Suitability. The degree to which users find the system to be suitable for the performance of their tasks.
* Understandability. The degree to which users find the system to be clear, legible, unambiguous, and comprehensible (especially during unusual situations).
* User Satisfaction. The degree to which users are satisfied with the system and consider it to be beneficial to them.

**(U)** **3.11.9.1 The system shall evoke in its users the feeling that its output is credible.**

(U) Specifically, at least 95% of a statistically valid sample of users shall rate the system’s output as being either highly correct or mostly correct on the following scale (highly correct, mostly correct, neutral, mostly incorrect, highly incorrect).

**(U)** **3.11.9.2 The system shall not require its users to perform numerous steps before they can begin using it.**

(U) Specifically, users shall be able to begin using the application to perform their tasks within 1 minute starting at least 90% of the time.

**(U)** **3.11.9.3 The system shall be easy for its users to remember how to use.**

(U) Specifically, at least 90% of a statistically valid sample of users shall rate the system as being either very easy to learn or easy to learn on the following scale (very easy to learn, easy to learn, neutral, difficult to learn, very difficult to learn.

**(U)** **3.11.9.4 The system’s user interface shall not require the user to either remember or copy information from one screen/webpage to another.**

(U) For example, the system may automatically reenter previously entered data on the new page, or else it may provide drop-down lists that allow users to select and enter valid choices.

**3.11.9.5 The system help functionality shall be easy to locate.**

**3.11.9.6 The system shall be easy for its users to use.**

(U) Specifically, at least 90% of a statistically valid sample of users shall rate the system as being either very easy to use or easy to use on the following scale (very easy to use, easy to use, neutral, difficult to use, very difficult to use).

**(U)** **3.11.9.7 The system shall be 508 compliant.**

(U) This compliance is according to the requirements specified under section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), and MIL-STD-1472.

**(U)** **3.11.9.8 The system shall improve the effectiveness of its users.**

Specifically, at least 90% of a statistically valid sample of users shall state that the system has made them either significantly more effective or more effective on the following scale (significantly more effective, more effective, neutral, less effective, significantly less effective).

**(U)** **3.11.9.9 The system shall minimize the errors made by its users.**

Specifically, at least 90% of a statistically valid sample of users shall state that the system has made them either significantly less error prone or less error prone on the following scale (significantly less error prone, less error prone, neutral, more error prone, more error prone).

**(U)** **3.11.9.10 The system shall minimize the errors made by its users by performing field validation to the maximum extent possible.**

**(U)** **3.11.9.11 The system’s user interface shall make it easy for users to navigate to where they want to go.**

(U) Specifically, at least 90% of a statistically valid sample of users shall rate the overall user interface as being either very easy to navigate or easy to navigate on the following scale (very easy to navigate, easy to navigate, neutral, difficult to navigate, very difficult to navigate).

**(U)** **3.11.9.12 Users of the system shall be able to navigate to major functions in one click from the main menu bar.**

**(U)** **3.11.9.13 The system shall enable users to retrieve data in the form they want.**

(U) Specifically, at least 90% of a statistically valid sample of users shall state that the system allows them to obtain data in the form they want.

**(U)** **3.11.9.14 The system shall enable users to download work product in the formats they need.**

(U) Specifically, the system shall allow users to download work product in .ppt, .pdf, and .xls formats.

**(U)** **3.11.9.15 The system shall be suitable for experienced users to use.**

(U) Specifically, at least 90% of a statistically valid sample of users with a minimum of 1 year of experience in Planning and 1 month of experience with the system shall state that it is either highly suitable or suitable for performing their tasks on the following scale (highly suitable, suitable, neutral, suitable, highly not suitable).

**(U)** **3.11.9.16 The system shall be suitable for novice users to use.**

(U) Specifically, at least 90% of a statistically valid sample of users with no prior experience in Planning and 2 months of experience with the system shall state that it is either highly suitable or suitable for performing their tasks on the following scale (highly suitable, suitable, neutral, suitable, highly not suitable).

**(U)** **3.11.9.17 The system’s user interface shall be clear to its users.**

(U) Specifically, at least 90% of a statistically valid sample of users shall rate the overall user interface as being either very clear or clear on the following scale (very clear, clear, neutral, unclear, very unclear).

**(U)** **3.11.9.18 The system’s help facilities shall be unambiguous to the users.**

(U) Specifically, at least 90% of a statistically valid sample of users shall rate the help facilities as being either very unambiguous or unambiguous on the following scale (very unambiguous, unambiguous, neutral, ambiguous, very ambiguous).

**(U)** **3.11.9.19 The system’s user-oriented error messages shall be easy for its users to understand.**

(U) Specifically, at least 90% of a statistically valid sample of trained users shall be able to interpret correctly 95% of a random selection of 10 of the system’s user-oriented error messages.

**(U)** **3.11.9.20 The system’s user guide shall be organized logically.**

(U) Specifically, at least 90% of a statistically valid sample of users shall rate the user guide as being either very logically organized or logically organized on the following scale (very logically organized, logically organized, neutral, illogically organized, very illogically organized).

**(U)** **3.11.9.21 The system’s installation and system administration guide shall be organized logically.**

(U) Specifically, at least 90% of a statistically valid sample of users shall rate the installation and system administration guide as being either very logically organized or logically organized on the following scale (very logically organized, logically organized, neutral, illogically organized, very illogically organized).

**(U)** **3.11.9.22 The system shall be beneficial to its users.**

(U) Specifically, at least 90% of a statistically valid sample of users shall rate the overall system as being either very beneficial or beneficial to performing their tasks on the following scale (very beneficial, beneficial, neutral, not beneficial, very unbeneficial).

## (U) Design and Construction Constraints

**(U)** **3.12.1 The system shall only provide email notification services if the host environment provides access to an email server for the system to use.**

**(U)** **3.12.2 The system design shall incorporate technology insertion concepts such that software components and hardware platforms can be modularly upgraded over time to take advantage of state-of-the-art technical advances in commercial information technology.**

**(U)** **3.12.4 The system shall be developed in Java to meet quality factors.**

(U) These factors are specified in section 3.11 of the SWIF SSS.

**(U)** **3.12.5 The system shall be capable of operating within the OZONE Widget Framework OWF environment.**

**(U)** **3.12.6 The system shall be capable of operating within the Intelligence Community Information Technology Enterprise (ICITE).**

## (U) Personnel-Related Requirements

(U) SWIF personnel security related requirements are defined in Section 3.8. The following subsection describes the system requirements for personnel.

**(U) 3.13.1 The systems users shall have experience in using browser-based applications.**

**(U)** **3.13.2 The system Administrative users shall have technical experience that exceeds the level of an average user.**

(U) Administrative users need the following skills:

* Experience using the operating system(s) that SWIF will be installed on
* Experience opening and issuing commands at the command line
* Administrator privileges for the hardware, operating system and database on which SWIF is installed
* Installed and configured a Mongo database
* Installed and configured Accumulo
* Installed and configured an application server
* Edited text files
* Ran scripts and executed SQL
* Performed simple debug tests on network and application connectivity
* Verified system configuration of the operating systems/VMs including RAM, CPU speed, remotely-mounted hard drives, etc.
* Ability to perform troubleshooting of application startup
* Knowledge and understanding of the meaning of terms such as localhost, domain name server (DNS), mount, SMTP, virtual machine (VM), PKI, SQL etc.
* Knowledge and understanding of PKI certificates and keystores.

## (U)Training-Related Requirements

(U) The following subsection describes the system requirements for training.

**(U) 3.14.1 The system users shall be trained initially via on-site training****.**

(U) Initial training will be as required.

**(U)** **3.14.2 Follow-on training for the system shall be via multiple avenues.**

(U) Follow-on training may include on-the-job, ancillary training by local personnel (trainers), or collaborative virtual capabilities [e.g., Defense Connect Online (DCO)].

**(U)** **3.14.3 The system shall not require users to take significant training to learn to use it to perform their tasks.**

(U) Specifically, the application shall enable at least 90% of a statistically valid sample of users to perform successfully their assigned tasks after receiving no more than 2 hours of instruction.

**(U)** **3.14.4 Training materials for the system shall include multiple products.**

(U) Examples of training materials include the following:

* Dictionary of terms and products (glossary)
* Description of functionality pertinent to General Users
* Description of processes involving SWIF Web Services system user operations
* Description of functionality pertinent to Privileged Users

**(U)** **3.14.5 The SWIF system training material shall be available via multiple means.**

(U) Examples of system training materials include the following:

* On-line (help topics, contextual help)
* On-line in downloadable files (to generate hardcopy materials)
* SWIF system development team members
* Instructor-led application hands-on training.

## (U) Logistic-Related Requirements

(U) The following subsection describes the system logistics-related requirements.

**(U)** **3.15.1 A Government-Contractor Integrated Product Team (IPT) shall deliver instructions detailing the procedures required for the use of any Commercial-off-the-Shelf (COTS) required by the SWIF system.**

(U) This includes installation and configuration.

**(U)** **3.15.2 A Government-Contractor Integrated Product Team (IPT) shall deliver instructions detailing the procedures required for the use of any Government-off-the-Shelf (GOTS) required by the SWIF system.**

(U) This includes installation and configuration.

**(U)** **3.15.3 A Government-Contractor Integrated Product Team (IPT) shall deliver listings of all required materials.**

(U) This includes COTS and GOTS.

**(U)** **3.15.4 A Government-Contractor Integrated Product Team (IPT) shall provide SWIF system maintenance.**

**(U)** **3.15.5 A Government-Contractor Integrated Product Team (IPT) shall provide software support for the SWIF system.**

**(U)3.15.6 The SWIF system shall generate reports showing information about the maintenance schedule.**

(U) This includes the following detailed and summary information:

* Routine maintenance schedules
* Non-routine maintenance schedule
* Upgrade maintenance schedule

(U) Implementation and operational priority for the schedule reports is in order stated above.

**(U)** **3.15.8 The system shall be implemented to allow Administrators to conduct remote administration.**

**(U)** **3.15.9 The deployment of the system shall not affect existing facilities already established to support special programs.**

**(U)** **3.15.10 The deployment of the system shall require dedicated equipment.**

**(U)** **3.15.11 The system shall xxx to prevent accidental destruction of the software.**

**(U)** **3.15.12 The system shall xxx to prevent accidental loss of data.**

## (U) Other Requirements

(U) This section is tailored out; no other requirements for SWIF have been identified.

## (U) Packaging and Labeling Requirements

(U) The following subsection describes the system requirements for packing and labeling.

**(U)** **3.17.1 The SWIF system shall be made available for third-party use using means determined by the SWIF Project Manager and the target network Security Manager.**

(U) Third party use includes supporting developers and installing media and/or using a communications path acceptable to the SWIF PM and the Security Manager.

**(U)** **3.17.2 All physical media shall be properly marked.**

(U) Proper marking includes the version number and security labeling requirements.

## (U) Precedence and Criticality of Requirements

(U) All requirements in this specification are of equal weight and criticality unless otherwise identified.

# (U) QUALIFICATION PROVISIONS

(U) Verification will consist of product inspection of delivered products to ensure compliance with all the requirements of this specification. A SWIF Test Plan will define specific qualification methods. The qualification method(s) will be specified for each requirement in the SWIF Test Procedures documents.

(U) Qualification of requirements will help ensure that the system under development achieves compliance. Qualification methods will consist of *demonstration*, *test*, *analysis*, and *inspection*. The SWIF Requirements Verification process will involve actual performance testing for each version release. The SWIF developer will verify conformance with the functional and performance requirements of Section 3 of this specification. The verification methods defined in this section will be applied at appropriate locations and levels of assembly up to and including a fully configured SWIF architecture. Verification levels, including Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E) are not yet defined.

(U) The following table summarizes the qualification method(s) appropriate for the system requirements in Section 3. The qualification method columns use the first letter (D, T, A, I, S) of the following methods prescribed in the SSS Data Item Description (DI-IPSC-81431A; see Section 2).

* Demonstration (D). The operation of the system, or part of the system, that relies on observable functional operation not requiring the use of instrumentation, special test equipment, or subsequent analysis. This method produces outputs that a human operator may directly observe and immediately evaluate.
* Test (T). The operation of the system, or part of the system, that relies on the collection and subsequent examination of data, possibly requiring the use of instrumentation or special test equipment.
* Analysis (A). The processing of accumulated data obtained from other qualification methods. Examples include interpolation or extrapolation of test results.
* Inspection (I). The visual inspection of system components, documentation, code, etc.
* Special (S). A verification test that does not fit one of the above categories; such cases require special explanations.

Table . (U) Qualification Provisions for Requirements

*[Table is* ***U//FOUO****]*

| **Para** | **ID** | **Requirement Statement** | **N/A** | **D** | **T** | **A** | **I** | **S** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **3. (U) Requirements** | | | | | | | | |
| **3.1 (U) Required States and Nodes** | | | | | | | | |
| **3.2.1 (U) System and Common Utilities** | | | | | | | | |
|  | 3.2.1.1 | (U) The system shall provide access using existing communications architectures. |  | D |  |  |  |  |
|  | 3.2.1.2 | (U) The SWIF software shall support existing networks that implement the TCP/IP communication protocol. |  | D |  |  |  |  |
|  | 3.2.1.3 | (U) The SWIF server shall support the use of RESTful Web Services for interfacing with external systems. |  | D |  |  |  |  |
|  | 3.2.1.4 | (U) Each system-generated entity shall have a unique identifier. |  | D |  |  |  |  |
|  | 3.2.1.5 | (U) The system shall support operations within multiple classified domains. |  | D |  |  |  |  |
|  | 3.2.1.6 | (U) The system shall be able to authenticate user access using external authentication servers. |  | D |  |  |  |  |
|  | 3.2.1.7 | (U) The system shall comply with the ICD 503 security requirements directed by the DAA. |  | D |  |  | I |  |
|  | 3.2.1.8 | (U) The system shall implement security features commensurate with the protection of the targeted deployment network requires. |  | D |  |  |  |  |
|  | 3.2.1.9 | (U) The system shall not allow the same user to be logged into the SWIF server simultaneously using the same browser type. |  | D |  |  |  |  |
|  | 3.2.1.10 | (U) The system shall provide a security service to control access to the system. |  | D |  |  |  |  |
|  | 3.2.1.11 | (U) The system shall control access to system functionality based on the user’s role. |  | D |  |  |  |  |
|  | 3.2.1.12 | (U) The system shall control access to system data based on the user’s attributes including clearance. |  | D |  |  |  |  |
|  | 3.2.1.13 | (U) The system shall implement security features commensurate with Protection Level (PL) 3 identified for the system interfaces for the deployed network. |  | D |  |  | I |  |
|  | 3.2.1.14 | (U) The system shall implement security features commensurate with the Availability Level Basis identified for the system interfaces for the deployed network. |  | D |  |  | I |  |
|  | 3.2.1.15 | (U) The system shall implement security features commensurate with the Integrity Level Basic identified for the system interfaces for the deployed network. |  | D |  |  | I |  |
|  | 3.2.1.16 | (U) The system shall be deployable to multiple container environments with minimal refactoring required. |  | D |  |  |  |  |
|  | 3.2.1.17 | (U) The system shall maintain content replication functionality that is standard with the operating system on a user’s workstation. |  | D |  |  |  |  |
|  | 3.2.1.18 | (U) The system shall provide for visualization capabilities. |  | D |  |  |  |  |
|  | 3.2.1.19 | (U) The system shall provide users a customizable display composed of widgets for interacting with data in the data store. |  | D |  |  |  |  |
|  | 3.2.1.20 | (U) The system shall provide a publish/subscribe capability whereby users can register to be notified of significant events related to topics of interest. |  | D |  |  |  |  |
|  | 3.2.1.21 | (U) The system shall make its information discoverable by external services. |  | D |  |  |  |  |
|  | 3.2.1.22 | (U) The system shall provide users the capability to set Discretionary Access to information stored in the system. |  | D |  |  |  |  |
|  | 3.2.1.23 | (U) The system shall provide conversion capabilities. |  | D | T |  |  |  |
|  | 3.2.1.24 | (U) The system shall provide eventing capabilities to support notifications between internal system components. |  |  |  |  | I |  |
|  | 3.2.1.25 | (U) The system shall provide for a status monitoring capability. |  | D |  |  |  |  |
|  | 3.2.1.26 | (U) The system shall provide the capability for Administrators to specify the conditions constituting an anomalous status that merits reporting. |  | D |  |  |  |  |
|  | 3.2.1.27 | (U) The system shall monitor the operational status of all the SWIF components. |  | D |  |  |  |  |
|  | 3.2.1.28 | (U) The system shall generate an audit report to the destinations specified by the Administrator upon detecting an anomalous operational status in any component. |  | D |  |  |  |  |
|  | 3.2.1.29 | (U) The system shall respond to an anomalous operational status as specified by the Administrator. |  | D |  |  |  |  |
|  | 3.2.1.30 | (U) The system shall collect generated audit data to support security event monitoring. |  | D |  |  |  |  |
|  | 3.2.1.31 | (U) The system shall monitor security events by analyzing collected audit data for anomalous conditions according to ISSO-defined rules to identify potential security violations. |  | D | T |  |  |  |
|  | 3.2.1.32 | (U) The system shall generate an audit report to the destinations specified by the ISSO upon detecting an anomalous security event. |  | D |  |  |  |  |
|  | 3.2.1.33 | (U) The system shall respond to imminent security violations as specified by the ISSO. |  | D |  |  |  |  |
| **3.2.1 (U) Visualization** | | | | | | | | |
|  | 3.2.2.1 | (U) The system shall include a user interface (UI) experience that includes widgets for general user functionality. |  | D |  |  |  |  |
|  | 3.2.2.2 | (U) The system shall allow the user to configure widgets into a workspace. |  | D |  |  |  |  |
|  | 3.2.2.3 | (U) The system shall allow the user to perform CRUDA operations for a workspace. |  | D |  |  |  |  |
|  | 3.2.2.4 | (U) The system shall allow the user to have multiple workspaces. |  | D |  |  |  |  |
|  | 3.2.2.5 | (U) The system shall include a map widget. |  | D |  |  |  |  |
|  | 3.2.2.6 | (U) The map widget shall be capable of displaying system-stored data. |  | D |  |  |  |  |
|  | 3.2.2.7 | (U) The map widget shall allow the user to generate geospatial shapes. |  | D |  |  |  |  |
|  | 3.2.2.8 | (U) The map widget shall be capable of rendering graphic overlays. |  | D |  |  |  |  |
|  | 3.2.2.9 | (U) The system shall include a multidimensional map visualization capability. |  | D |  |  |  |  |
|  | 3.2.2.10 | (U) Map-based icons shall be distinguishable by the type of data. |  | D |  |  |  |  |
|  | 3.2.2.11 | (U) The system shall be able to display map-based icons using a common display standard. |  | D |  |  |  |  |
|  | 3.2.2.12 | (U) The system shall provide the capability for the user to mouse over an icon displayed on a map overlay to view a summary of information about the icon. |  | D |  |  |  |  |
|  | 3.2.2.13 | (U) The system shall provide the capability for the user to select an icon displayed on a map overlay to view detailed information about the object in a separate window or widget. |  | D |  |  |  |  |
|  | 3.2.2.14 | (U) The system shall support the OpenGIS Web Map Service (WMS) standard for requesting geo-registered map artifacts. |  | D |  |  |  |  |
|  | 3.2.2.15 | (U) The system shall support the ability to select a map server by entering a Map Server URL. |  | D |  |  |  |  |
|  | 3.2.2.16 | (U) The system shall support the OpenGIS Web Features Service (WFS) standard for requesting feature data. |  | D |  |  |  |  |
|  | 3.2.2.17 | (U) The system shall support user selection of a map server from a list of multiple candidate servers for display. |  | D |  |  |  |  |
|  | 3.2.2.18 | (U) The system shall be capable of operating as widgets within widget frameworks. |  | D |  |  |  |  |
|  | 3.2.2.19 | (U) System widgets shall be capable of operating within different widget frameworks. |  | D |  |  |  |  |
|  | 3.2.2.20 | (U) The SWIF server shall support commonly accepted Web technologies. |  | D |  |  |  |  |
|  | 3.2.2.21 | (U) SWIF widgets shall interface with the SWIF server using commonly accepted Web technologies. |  | D |  |  |  |  |
|  | 3.2.2.22 | (U) The system shall provide a widget management environment that allows each user to have at least one workspace. |  | D |  |  |  |  |
|  | 3.2.2.23 | (U) The system shall include a Search widget to access data. |  | D |  |  |  |  |
|  | 3.2.2.24 | (U) The system shall include a Search widget that allows users to access stored capabilities. |  | D |  |  |  |  |
|  | 3.2.2.25 | (U) The system shall include a Search widget that allows users to search for other users. |  | D |  |  |  |  |
|  | 3.2.2.26 | (U) The system shall include a data monitoring widget that allows users to view data feed status. |  | D |  |  |  |  |
|  | 3.2.2.27 | (U) The system shall include a collaboration widget. |  | D |  |  |  |  |
|  | 3.2.2.28 | (U) The system shall include a link analysis widget. |  | D |  |  |  |  |
|  | 3.2.2.29 | (U) The system shall include a graph visualization widget. |  | D |  |  |  |  |
|  | 3.2.2.30 | (U) The system shall include a data import widget. |  | D |  |  |  |  |
|  | 3.2.2.31 | (U) The system shall provide a timeline widget. |  | D |  |  |  |  |
|  | 3.2.2.32 | (U) The system shall provide an operations clock tool. |  | D |  |  |  |  |
|  | 3.2.2.33 | (U) The system shall provide a decision matrix widget. |  | D |  |  |  |  |
| **3.2.3 (U) Roles and User Account Management** | | | | | | | | |
|  | 3.2.3.1 | (U) The system shall provide a Web-based user interface (UI) to support user account management (UAM) functionality. |  | D |  |  |  |  |
|  | 3.2.3.2 | (U) The system shall provide the capability to use user account privileges to manage user access. |  | D |  |  |  |  |
|  | 3.2.3.3 | (U) The system shall employ user roles that restrict user access to system functionality based on assigned roles. |  | D |  |  |  |  |
|  | 3.2.3.4 | (U) The system shall provide a set of roles to allow users to have system access. |  | D |  |  |  |  |
|  | 3.2.3.5 | (U) The system shall allow adding additional roles without requiring a major redesign of the system. |  | D |  |  | I |  |
|  | 3.2.3.6 | (U) The system shall provide the capability to change a user’s assigned roles. |  | D |  |  |  |  |
|  | 3.2.3.7 | (U) The system shall provide the capability to reset the passwords for existing user accounts. |  | D |  |  |  |  |
|  | 3.2.3.8 | (U) The system shall notify the user via that user’s account-associated email address when the user’s password has changed. |  | D |  |  |  |  |
|  | 3.2.3.9 | (U) The system shall provide a user account workflow to manage account creation. |  | D |  |  |  |  |
|  | 3.2.3.10 | (U) User accounts in the system shall be capable of being in only one state at any one time. |  | D |  |  |  |  |
|  | 3.2.3.11 | (U) The system shall support multiple states. |  | D |  |  |  |  |
|  | 3.2.3.12 | (U) The system shall retain all user accounts regardless of their current state. |  | D |  |  |  |  |
|  | 3.2.3.13 | (U) The system shall provide the capability for viewing user accounts based on the account state. |  | D |  |  |  |  |
|  | 3.2.3.14 | (U) The system shall assign a unique identifier to each user account. |  | D |  |  |  |  |
|  | 3.2.3.15 | (U) The system shall require the use of strong passwords. |  | D |  |  |  |  |
|  | *[3.2.3.16* | *(U) not used; added to 3.2.3.15]* | *N/A* |  |  |  |  |  |
|  | 3.2.3.17 | (U) The system shall reject a password if the user tries to save a password that does not meet the strong password requirement. |  | D |  |  |  |  |
|  | 3.2.3.18 | (U) The system shall lock a user account if the user fails three successive login attempts within a given timeframe. |  | D |  |  |  |  |
|  | 3.2.3.19 | (U) The system shall allow only Administrators to unlock user accounts. |  | D |  |  |  |  |
|  | 3.2.3.20 | (U) The system shall age user account passwords with a maximum allowed usage time limit set as a system configuration item with default to one year (365 days). |  | D |  |  |  |  |
|  | 3.2.3.21 | (U) If a user’s current password has aged beyond three months (90 days), the system shall automatically lock a user account, preventing the user access until the user changes the password for the account. |  | D |  |  |  |  |
|  | 3.2.3.22 | (U) The system shall notify a user each time the user attempts to login if the account password is set to expire, beginning 10 days prior to its expiration. |  | D |  |  |  |  |
|  | 3.2.3.23 | (U) The system shall provide the capability to input specific user information during user account creation. |  | D |  |  |  |  |
|  | 3.2.3.24 | (U) The system shall not allow the user to access the account during the approval process. |  | D |  |  |  |  |
|  | 3.2.3.25 | (U) The system shall allow the user to change specific values of the user’s account information. |  | D |  |  |  |  |
|  | 3.2.3.26 | (U) The system shall require all login IDs to be unique. |  | D |  |  |  |  |
|  | 3.2.3.27 | (U) The system shall notify the user, using the user’s email address on file in the account for the network, that a new account has been created for them and is ready for use. |  | D |  |  |  |  |
|  | 3.2.3.28 | (U) The system shall separately notify the user, using the user’s contact email address for the network, of the new temporary account password. |  | D |  |  |  |  |
|  | 3.2.3.29 | (U) The system shall provide a strong password auto-generation capability to assign new passwords for user accounts. |  | D |  |  |  |  |
|  | 3.2.3.30 | (U) The system shall allow the user to use the password auto-generation capability to generate a new password for the user account. |  | D |  |  |  |  |
|  | 3.2.3.31 | (U) The system shall allow the user to change the user’s system-generated temporary password upon their first login after password reset. |  | D |  |  |  |  |
|  | 3.2.3.32 | (U) The system shall allow the Site Administrator to configure the number of days after creation of a new account the password will expire if the user does not log in. |  | D |  |  |  |  |
|  | 3.2.3.33 | (U) The system shall require all users to revalidate their user account information as part of account renewal in accordance with the renewal time frame within the user account. |  | D |  |  |  |  |
|  | 3.2.3.34 | (U) The system shall notify users of their required renewal thirty (30) days prior to their account expiring. |  | D |  |  |  |  |
|  | 3.2.3.35 | (U) The system shall automatically lock user accounts that are not renewed in accordance with the renewal time frame within their user account. |  | D |  |  |  |  |
|  | 3.2.3.36 | (U) The system shall provide the capability for the ISSO to set the renewal time frame for each user account as an individually configurable value. |  | D |  |  |  |  |
|  | 3.2.3.37 | (U) The system shall require account renewal re-approval by revalidation of security clearances with associated accesses by the user’s security officer. |  | D |  |  |  |  |
|  | 3.2.3.38 | (U) The system shall provide a capability dynamically to enforce “least privilege” functionality for individual users. |  | D |  |  |  |  |
|  | 3.2.3.39 | (U) The system shall provide the capability to support public key infrastructure (PKI) certificates. |  | D |  |  |  |  |
|  | 3.2.3.40 | (U) The system shall allow the user to use external credentials for system access. |  | D |  |  |  |  |
|  | 3.2.3.41 | (U) The system shall support the concept of an “alias” to hide the true name of the user. |  | D |  |  |  |  |
|  | 3.2.3.42 | (U) The system shall provide the capability to disable system roles. |  | D |  |  |  |  |
| **3.2.4 (U) Groups** | | | | | | | | |
|  | 3.2.4.1 | (U) The system shall provide the capability for users to manage groups of users. |  | D |  |  |  |  |
|  | 3.2.4.2 | (U) When searching for users to associate to the group, the system shall filter search results to display only those users whose attributes (including clearance) satisfy the classification level set for the group. |  | D |  |  |  |  |
|  | 3.2.4.3 | (U) The system’s notification capability shall support notifications. |  | D |  |  |  |  |
|  | 3.2.4.4 | (U) The system shall provide the capability to hide the existence of a group. |  | D |  |  |  |  |
|  | 3.2.4.5 | (U) The system shall allow groups to be composed of individuals from multiple organizations. |  | D |  |  |  |  |
|  | 3.2.4.6 | (U) The system shall allow groups to perform CRUDA operations for a workspace. |  | D |  |  |  |  |
| **3.2.5 (U) Search** | | | | | | | | |
|  | 3.2.5.1 | (U) The system shall provide the capability for a user to search for information stored in the SWIF data store. |  | D |  |  |  |  |
|  | 3.2.5.2 | (U) The system shall provide the capability for a user to search for user information residing in data stores external to SWIF. |  | D |  |  |  |  |
|  | 3.2.5.3 | (U) The system shall restrict the ability to search for user information residing in data stores external to SWIF to roles configured by an Administrator. |  | D |  |  |  |  |
|  | 3.2.5.4 | (U) The system shall provide the capability for a user to save search results. |  | D |  |  |  |  |
|  | 3.2.5.5 | (U) The system shall provide a keyword search capability. |  | D |  |  |  |  |
|  | 3.2.5.6 | (U) The system shall provide a map interface for users to conduct geospatial searches. |  | D |  |  |  |  |
|  | 3.2.5.7 | (U) The system shall provide the capability for a user to conduct a geospatial search by entering coordinates. |  | D |  |  |  |  |
|  | 3.2.5.8 | (U) The system shall provide the capability for a user to conduct a geospatial search by entering coordinates. |  | D |  |  |  |  |
|  | 3.2.5.9 | (U) The system shall support multiple coordinate types. |  | D |  |  |  |  |
|  | 3.2.5.10 | (U) The system shall provide the capability for exporting search results into a tab delimited ASCII text file. |  | D |  |  |  |  |
|  | 3.2.5.11 | (U) The system shall remove duplicate results from search results prior to displaying the results to the user. |  | D |  |  |  |  |
|  | 3.2.5.12 | (U) The system shall provide the capability for a user to specify the maximum number of results for the system to display per page. |  | D |  |  |  |  |
|  | 3.2.5.13 | (U) The system shall provide the capability, in search results displays, for the user to view the number of total matches found by the search. |  | D |  |  |  |  |
|  | 3.2.5.14 | (U) The system shall sort the entire search results set when data is sorted. |  | D |  |  |  |  |
|  | 3.2.5.15 | (U) The system shall provide the capability for the user, after a result set is returned, to sort the results by selecting the column label of the data fields displayed in the results set. |  | D |  |  |  |  |
|  | 3.2.5.16 | (U) The system shall allow the user to select results for removal from a search results set. |  | D |  |  |  |  |
| **3.2.6 (U) Workflows and Queues** | | | | | | | | |
|  | 3.2.6.1 | (U) The system shall provide for a workflow capability. |  | D |  |  |  |  |
|  | 3.2.6.2 | (U) The system shall provide for a set of factory-delivered predefined workflows. |  | D |  |  |  |  |
|  | 3.2.6.3 | (U) The system shall provide the capability for Administrators to choose from a set of workflows. |  | D |  |  |  |  |
|  | 3.2.6.4 | (U) The system shall provide the capability for Group Managers to assign workflow entities to users assigned to their queue as part of the workflow process. |  | D |  |  |  |  |
|  | 3.2.6.5 | (U) The system shall be capable of automatically routing workflow tasks to the appropriate queue based on workflow. |  | D |  |  |  |  |
|  | 3.2.6.6 | (U) The system shall provide the capability to route system work products in workflow on which users can work. |  | D |  |  |  |  |
|  | 3.2.6.7 | (U) The system shall provide the capability for a user to view the workflow entity that is in a queue for which the user is assigned. |  | D |  |  |  |  |
|  | 3.2.6.8 | (U) The system shall provide the capability for Administrators to assign Group Managers to queues in a workflow. |  | D |  |  |  |  |
|  | 3.2.6.9 | (U) The system shall provide the capability for multiple users to access a Group’s workflow process simultaneously. |  | D |  |  |  |  |
|  | 3.2.6.10 | (U) The system shall allow entities to move from one activity to the next activity based on the group’s workflow process. |  | D |  |  |  |  |
|  | 3.2.6.11 | (U) The system shall provide notifications to users within a workflow based on status information. |  | D |  |  |  |  |
|  | 3.2.6.12 | (U) The system shall provide the capability for a user to save a workflow. |  | D |  |  |  |  |
|  | 3.2.6.13 | (U) The system shall provide the capability for Group Managers to view their queues. |  | D |  |  |  |  |
|  | 3.2.6.14 | (U) The system shall provide the user with status on the user’s workflow execution processes. |  | D |  |  |  |  |
|  | 3.2.6.15 | (U) The system shall be capable of storing multiple workflows. |  | D |  |  |  |  |
|  | 3.2.6.16 | (U) The system shall provide the capability for a user to view the workflow history of a workflow entity as it works through the end-to-end workflow process. |  | D |  |  |  |  |
|  | 3.2.6.17 | (U) The system shall provide the capability for users assigned to a workflow to be able to view the Workflow History for all products. |  | D |  |  |  |  |
|  | 3.2.6.18 | (U) The system shall provide the capability for a queue member to set notifications upon receipt of new entities available for work in the member’s assigned queues. |  | D |  |  |  |  |
|  | 3.2.6.19 | (U) The system shall provide the capability for a workflow manager to configure queues to support workflow. |  | D |  |  |  |  |
|  | 3.2.6.20 | (U) The system shall provide the capability for an Administrator to perform queue management functions. |  | D |  |  |  |  |
|  | 3.2.6.21 | (U) The system shall provide the capability for Group Managers to restrict workflow access to specific users. |  | D |  |  |  |  |
|  | 3.2.6.22 | (U) The system shall allow the Group Manager to lock write access to a workflow entity. |  | D |  |  |  |  |
| **3.2.7 (U) Import/Export** | | | | | | | | |
|  | 3.2.7.1 | (U) The system shall provide the capability for a user to import data into the SWIF data store. |  | D |  |  |  |  |
|  | 3.2.7.2 | (U) The system shall provide the capability for a user to export data from the SWIF data store. |  | D |  |  |  |  |
|  | 3.2.7.3 | (U) The system shall have the capability to receive automated online data ingest of sources. |  | D |  |  |  |  |
|  | 3.2.7.4 | (U) The system shall provide the capability to stage ingested data in temporary storage for review before permanent storage. |  | D |  |  |  |  |
|  | 3.2.7.5 | (U) The system shall provide users the capability to set and the accessibility of imported information. |  | D |  |  |  |  |
|  | 3.2.7.6 | (U) The system shall include accessibility information for exporting information. |  | D |  |  |  |  |
|  | 3.2.7.7 | (U) The system shall provide a temporary storage area for imported data that will serve as a “quarantine” area until the data can be reviewed when there is no anti-virus scan available. |  | D |  |  |  |  |
|  | 3.2.7.8 | (U) The system shall provide a capability to convert imported CSV files to SWIF CDM format. |  | D |  |  |  |  |
|  | 3.2.7.9 | (U) The system shall provide a capability that allows imported data to be stored in the SWIF data store. |  | D |  |  |  |  |
|  | 3.2.7.10 | (U) The system shall provide a capability to import Capabilities. |  | D |  |  |  |  |
|  | 3.2.7.11 | (U) The system shall provide a capability to export Capabilities. |  | D |  |  |  |  |
| **3.2.8 (U) Named Areas of Interest** | | | | | | | | |
|  | 3.2.8.1 | (U) The system shall provide the capability for users to perform CRUDA operations for Named Areas of Interest (NAIs). |  | D |  |  |  |  |
|  | 3.2.8.2 | (U) The default discretionary access of a Named Area of Interest (NAI) shall be private. |  | D |  |  |  |  |
|  | 3.2.8.3 | (U) The system shall support Named Areas of Interest (NAIs) represented by geodetic coordinates. |  | D |  |  |  |  |
|  | 3.2.8.4 | (U) The system shall provide the capability for users to create a Named Area of Interest (NAI) through text entry of coordinates. |  | D |  |  |  |  |
|  | 3.2.8.5 | (U) The system shall provide the capability for users to create a Named Area of Interest (NAI) by dropping a point or drawing a line or polygon on a geodetic map display. |  | D |  |  |  |  |
|  | 3.2.8.6 | (U) The system shall provide the capability to associate Named Areas of Interest (NAIs) to other entities in the system. |  | D |  |  |  |  |
| **3.2.9 (U) Analytic Tools** | | | | | | | | |
|  | 3.2.9.1 | (U) The system shall provide a text analytics capability. |  | D |  |  |  |  |
|  | 3.2.9.2 | (U) The system shall provide a heat map analytic capability. |  | D |  |  |  |  |
|  | 3.2.9.3 | (U) The system shall provide an analysis of competing hypothesis capability. |  | D |  |  |  |  |
|  | 3.2.9.4 | (U) The system shall provide a Geographic Information System (GIS) tool. |  | D |  |  |  |  |
|  | 3.2.9.5 | (U) The system shall provide a statistical analysis tool. |  | D |  |  |  |  |
|  | 3.2.9.6 | (U) The system shall provide predictive models. |  | D |  |  |  |  |
|  | 3.2.9.7 | (U) The system shall provide influence diagramming capability. |  | D |  |  |  |  |
|  | 3.2.9.8 | (U) The system shall provide scientific models. |  | D |  |  |  |  |
|  | 3.2.9.9 | (U) The system shall provide engineering models. |  | D |  |  |  |  |
|  | 3.2.9.10 | (U) The system shall provide system dynamic models. |  | D |  |  |  |  |
|  | 3.2.9.11 | (U) The system shall provide simulation models. |  | D |  |  |  |  |
| **3.2.10 (U) Production** | | | | | | | | |
|  | 3.2.10.1 | (U) The system shall provide the capability to generate products using data stored in the system. |  | D |  |  |  |  |
|  | 3.2.10.2 | (U) The system shall provide users the ability to develop reports as a result of the analytical operations performed using the domain-specific application. |  | D |  |  |  |  |
|  | 3.2.10.3 | (U) The system shall provide the capability for users to create customized views that can be made into product templates to suit formatting requirements. |  | D |  |  |  |  |
|  | 3.2.10.4 | (U) The system shall provide the capability for users to generate products in multiple formats. |  | D |  |  |  |  |
|  | 3.2.10.5 | (U) The system shall generate all products in compliance with classification requirements of the deployment network. |  | D |  |  |  |  |
|  | 3.2.10.6 | (U) The system shall provide the capability for users to set the classification of a product. |  | D |  |  |  |  |
|  | 3.2.10.7 | (U) The system shall provide the capability for users to set the classification of a product template. |  | D |  |  |  |  |
| **3.2.11 (U) Notification** | | | | | | | | |
|  | 3.2.11. | (U) The system shall provide a notification capability. |  | D |  |  |  |  |
|  | 3.2.11. | (U) The system shall be capable of sending notifications via multiple delivery paths, with email being the default path. |  | D |  |  |  |  |
|  | 3.2.11. | (U) The system shall provide the capability for users to set notification preferences. |  | D |  |  |  |  |
|  | 3.2.11. | (U) The system shall support the ability to select a notification choice for a supported event via a supported channel. |  | D |  |  |  |  |
| **3.2.12 (U) Subscription** | | | | | | | | |
|  | 3.2.12.1 | (U) The system shall provide the capability for a user to set up a feed that displays events relevant to the user’s specified needs. |  | D |  |  |  |  |
|  | 3.2.12.2 | (U) The system shall allow a user to follow a system event. |  | D |  |  |  |  |
|  | 3.2.12.3 | (U) The system shall provide a capability to follow system events. |  | D |  |  |  |  |
|  | 3.2.12.4 | (U) Any time a change is made to a followed entity, the system shall make that change appear on the user’s feed. |  | D |  |  |  |  |
|  | 3.2.12.5 | (U) The system shall provide the capability for a user to subscribe to system entities. |  | D |  |  |  |  |
|  | 3.2.12.6 | (U) The system shall provide the capability for a user to subscribe to system work products. |  | D |  |  |  |  |
|  | 3.2.12.7 | (U) The system shall provide the capability for a user to set criteria which, when met, will result in the system notifying the user. |  | D |  |  |  |  |
| **3.2.13 (U) Audit** | | | | | | | | |
|  | 3.2.13.1 | (U) The system shall record significant events in audit records. |  | D |  |  |  |  |
|  | *[3.2.13.2* | *(U) not used; added to 3.2.13.1]* | *N/A* |  |  |  |  |  |
|  | 3.2.13.3 | (U) The system shall provide a Web-based user interface (UI) for viewing audit information. |  | D |  |  |  |  |
|  | 3.2.13.4 | (U) The system shall provide auditing of individual accountability. |  | D |  |  |  |  |
|  | 3.2.13.5 | (U) The system shall ensure all audit records include information to allow administrators the ability to evaluate the audited event. |  | D |  |  |  |  |
|  | 3.2.13.6 | (U) The system shall provide protection of the contents of audit trails against unauthorized use. |  | D |  |  |  |  |
|  | 3.2.13.7 | (U) The system shall provide the capability to allow only those users with the appropriate role access to Audit information. |  | D |  |  |  |  |
|  | 3.2.13.8 | (U) The system shall restrict all historical logs in such a manner that they cannot be edited by a general user. |  | D |  |  |  |  |
| **3.2.14 (U) Usage and Performance Analytics** | | | | | | | | |
|  | 3.2.14.1 | (U) The system shall limit access to usage and performance analytics (UPA) by role. |  | D |  |  |  |  |
|  | 3.2.14.2 | (U) The system shall provide a Web-based user interface (UI) to support usage and performance analytics (UPA). |  | D |  |  |  |  |
|  | 3.2.14.3 | (U) The system shall provide the capability for an authorized user to view usage and performance analytics (UPA) information for a specified period. |  | D | T |  |  |  |
| **3.2.15 (U) System Configuration** | | | | | | | | |
|  | 3.2.15.1 | (U) The system shall provide a Web-based user interface (UI) to support System Configuration functionality. |  | D |  |  |  |  |
|  | 3.2.15.2 | (U) The system shall restrict access to application configuration settings to privileged users designated as application administrators. |  | D |  |  |  |  |
|  | 3.2.15.3 | (U) The system shall provide the capability for an administrator to set configurations. |  | D |  |  |  |  |
|  | 3.2.15.4 | (U) The system shall provide the capability for Administrators to set the E-Mail configuration preferences. |  | D |  |  |  |  |
|  | 3.2.15.5 | (U) The system shall provide the capability for Administrators to set map configuration preferences. |  | D |  |  |  |  |
| **3.2.16 (U) User Preferences** | | | | | | | | |
|  | 3.2.16.1 | (U) The system shall allow a user to configure the user’s preferences for data display. |  | D |  |  |  |  |
|  | 3.2.16.2 | (U) The system shall allow a user to configure the user’s preferences for notifications. |  | D |  |  |  |  |
|  | 3.2.16.3 | (U) The system shall allow a user to update only the user’s own user profile information. |  | D |  |  |  |  |
|  | 3.2.16.4 | (U) The system shall allow a user with the role of Administrator to update user preferences for any user. |  | D |  |  |  |  |
|  | 3.2.16.5 | (U) The system shall provide a Web-based user interface (UI) for viewing user preferences. |  | D |  |  |  |  |
|  | 3.2.16.6 | (U) The system shall allow each user to select the type of map-based icons for the user’s map displays. |  | D |  |  |  |  |
|  | 3.2.16.7 | (U) The system user interface (UI) shall allow a user to configure the user’s preferences for default settings. |  | D |  |  |  |  |
|  | 3.2.16.8 | (U) The system shall allow a group to configure the display preferences that can then be used by members of the group. |  | D |  |  |  |  |
|  | 3.2.16.9 | (U) The system shall allow a user to save the user’s preferences for workspace settings. |  | D |  |  |  |  |
| **3.2.17 (U) User Interface** | | | | | | | | |
|  | 3.2.17.1 | (U) The system shall provide a browser-based user interface (UI) to execute system functions. |  | D |  |  |  |  |
|  | 3.2.17.2 | (U) The system user interface (UI) presented to the user shall be based on the user’s role. |  | D |  |  |  |  |
|  | 3.2.17.3 | (U) The system’s Web-based user interface (UI) shall not rely upon the browser back button for navigation. |  | D |  |  |  |  |
|  | 3.2.17.4 | (U) The system’s Web-based user interface (UI) shall use consistent naming conventions for action buttons. |  | D |  |  |  |  |
|  | 3.2.17.5 | (U) The system shall support forms with consistent behavior. |  | D |  |  |  |  |
|  | 3.2.17.6 | (U)The system shall use a CLOSE button (if in view mode) to return to previous page. |  | D |  |  |  |  |
|  | 3.2.17.7 | (U) The system shall provide a flag for user action to populate mandatory fields that are not populated. |  | D |  |  |  |  |
|  | 3.2.17.8 | (U) When a field fails validity checking, the system will flag the invalid data values within the template prompting user correction of the invalid data. |  | D |  |  |  |  |
|  | 3.2.17.9 | (U) The system shall allow the selection of a single item obtained from the results of a search, displaying its details in a new window. |  | D |  |  |  |  |
|  | 3.2.17.10 | (U) The system shall allow the selection of the details of associated entities. |  | D |  |  |  |  |
|  | 3.2.17.11 | (U) If a user entry must be one of several defined items, then the system shall present the user with the list of items from which to select the entry. |  | D |  |  |  |  |
|  | 3.2.17.12 | (U) The system shall have a consistent layout of the fields regardless of the mode for pages with more than one mode. |  |  |  |  |  |  |
|  | 3.2.17.13 | (U) The system user interface (UI) shall provide the capability for the user to associate entities using a drag-and-drop metaphor. |  | D |  |  |  |  |
|  | 3.2.17.14 | (U) The system shall use display tags that indicate the presence of mandatory field in a consistent manner for all user-entered fields within the system. |  | D |  |  |  |  |
|  | 3.2.17.15 | (U) The system shall use a consistent markup format on user interface (UI) features to indicate when a selection is not available to the user. |  | D |  |  |  |  |
|  | 3.2.17.16 | (U) The system shall contain an automatic timeout capability. |  | D |  |  |  |  |
|  | 3.2.17.17 | (U) The system shall provide error message windows with consistent behavior. |  | D |  |  |  |  |
|  | 3.2.17.18 | (U) The system shall provide Save functionality within the browser-based user interface (UI). |  | D |  |  |  |  |
|  | 3.2.17.19 | (U) The system shall support field validation. |  | D |  |  |  |  |
|  | 3.2.17.20 | (U) The system shall display tags that indicate the presence of mandatory fields in a consistent manner for all user data entry capabilities within the system. |  | D |  |  |  |  |
|  | 3.2.17.21 | (U) Use a consistent format and markup on user interface features to indicate when a function/field is not available to the user. |  | D |  |  |  |  |
|  | 3.2.17.22 | (U) The system shall provide for the following general behavior for the system’s work products. |  | D |  |  |  |  |
|  | 3.2.17.23 | (U) The system shall provide a defined set of capabilities for the user interface (UI) to support Search. |  | D |  |  |  |  |
|  | 3.2.17.24 | (U) The system shall provide the ability to color-code settings in the user interface (UI). |  | D |  |  |  |  |
|  | 3.2.17.25 | (U) The system shall provide a feedback mechanism to the user to indicate the system is processing the user-requested action if the transaction requires more than two (2) seconds to respond. |  | D |  |  |  |  |
|  | 3.2.17.26 | (U) The system’s Web-based user interface (UI) shall not require Java to be installed in the user’s browser. |  | D |  |  |  |  |
|  | 3.2.17.27 | (U) The system’s Web-based user interface (UI) shall not use Java applets. |  | D |  |  |  |  |
| **3.2.18 (U) Database** | | | | | | | | |
|  | 3.2.18.1 | (U) The system shall incorporate data storage capabilities that support transactions using, at a minimum, a v3 Java Database Connectivity (JDBC) driver. |  |  |  |  | I |  |
|  | 3.2.18.2 | (U) The system database shall support protection of classified data. |  | D |  |  | I |  |
|  | 3.2.18.3 | (U) When accessing a non-SQL database, the system shall incorporate a relational database that supports transactions. |  |  |  |  | I |  |
|  | 3.2.18.4 | (U) The system database shall permit internal application connections for the purposes of managing system information. |  |  |  |  | I |  |
|  | 3.2.18.5 | (U) The system database shall provide the capability to store audit information. |  | D |  |  |  |  |
|  | 3.2.18.6 | (U) The system database shall provide the capability to store work product information. |  | D |  |  |  |  |
|  | 3.2.18.7 | (U) The system database shall provide the capability to store entity information. |  | D |  |  |  |  |
|  | 3.2.18.8 | (U) The system database shall provide the capability to store notification messages. |  | D |  |  |  |  |
|  | 3.2.18.9 | (U) The system database shall provide the capability to store user account information. |  | D |  |  |  |  |
|  | 3.2.18.10 | (U) The system database shall provide the capability to store user preferences. |  | D |  |  |  |  |
|  | 3.2.18.11 | (U) The system database shall provide the capability to store list of value (lookup) types of data for use across the application to ensure consistency. |  | D |  |  |  |  |
|  | 3.2.18.12 | (U) The system database shall provide the capability to store canned searches for use by all system users. |  | D |  |  |  |  |
|  | 3.2.18.13 | (U) The system database shall provide the capability to store user-defined searches for later use by the user. |  | D |  |  |  |  |
|  | 3.2.18.14 | (U) The system database shall provide the capability to store a defined workflow. |  | D |  |  |  |  |
|  | 3.2.18.15 | (U) The system database shall provide the capability to store the user work queue data. |  | D |  |  |  |  |
|  | 3.2.18.16 | (U) The system database shall provide the capability to store the group work queue data. |  | D |  |  |  |  |
|  | 3.2.18.17 | (U) The system database shall provide the capability to store simulation data. |  | D |  |  |  |  |
|  | 3.2.18.18 | (U) The system database shall provide the capability to store group account information. |  | D |  |  |  |  |
|  | 3.2.18.19 | (U) The system database shall provide the capability to store product templates. |  | D |  |  |  |  |
|  | 3.2.18.20 | (U) The system database shall provide the capability to store site-level system configuration information. |  | D |  |  |  |  |
|  | 3.2.18.21 | (U) The system database shall provide the capability to store copies of all information transmitted to external systems. |  | D |  |  |  |  |
|  | 3.2.18.22 | (U) The system database shall provide for online access to all stored data information, through the application, for a minimum of five years. |  | D |  |  |  |  |
|  | 3.2.18.23 | (U) The system database shall associate stored data to the user who performed CRUDA operations on it. |  | D |  |  |  |  |
|  | 3.2.18.24 | (U) The system database shall store user widget settings for each workspace. |  | D |  |  |  |  |
| **3.2.19 (U) Installation and Configuration** | | | | | | | | |
|  | 3.2.19.1 | (U) The system shall be developed such that it can be built with a single command. |  | D |  |  |  |  |
|  | 3.2.19.2 | (U) The system shall be installable with simple scripts. |  | D |  |  |  |  |
|  | 3.2.19.3 | (U) The system shall provide test scripts to ensure the system is installed correctly. |  |  | T |  |  |  |
|  | 3.2.19.4 | (U) The system shall allow the configuration of key system settings without requiring a software release. |  | D |  |  |  |  |
|  | 3.2.19.5 | (U) The system shall provide the ability to specify server connection information in a configuration file. |  | D |  |  |  |  |
|  | 3.2.19.6 | (U) The system shall support the use of scripts to create required database artifacts. |  | D |  |  | I |  |
|  | 3.2.19.7 | (U) The system shall support the use of scripts to load initialization data into the database. |  | D |  |  |  |  |
|  | 3.2.19.8 | (U) The install process shall be documented. |  |  |  |  | I |  |
|  | 3.2.19.9 | (U) The system shall provide a capability for its initialization. |  | D |  |  |  |  |
|  | 3.2.19.10 | (U) The system shall provide the capability for an orderly controlled shutdown of operations. |  | D |  |  |  |  |
|  | 3.2.19.11 | (U) The system shall provide the capability to update configuration setting for selected server-side functionality. |  | D |  |  |  |  |
|  | 3.2.19.12 | (U) The system shall be able to perform a backup operation on request. |  | D |  |  |  |  |
|  | 3.2.19.13 | (U) The system shall be able to perform a restore operation on request. |  | D |  |  |  |  |
|  | 3.2.19.14 | (U) The system shall be able to perform a backup of security-relevant functions on request. |  | D |  |  |  |  |
|  | 3.2.19.15 | (U) The system shall be able to restore, on request, the security-relevant functions up to the last backup archive. |  | D |  |  |  |  |
|  | 3.2.19.16 | (U) The system shall be capable of being restored to the last known secure configuration through the application of the recorded changes to security-relevant functions. |  | D |  |  |  |  |
| **3.2.20 (U) Help** | | | | | | | | |
|  | 3.2.20.1 | (U) The system shall provide an online help capability. |  | D |  |  |  |  |
|  | 3.2.20.2 | (U) The system shall provide the capability for privileged users to access contact information. |  | D |  |  |  |  |
|  | 3.2.20.3 | (U) The system shall provide on-line documentation. |  | D |  |  |  |  |
|  | 3.2.20.4 | (U) The system shall provide the capability for on-line problem reporting. |  | D |  |  |  |  |
| **3.2.21 (U) Deployment** | | | | | | | | |
|  | 3.2.21.1 | (U) The system shall be capable of being deployed in a high assurance (HA) deployment configuration. |  | D |  |  |  |  |
|  | 3.2.21.2 | (U) The system shall be capable of supporting Elastic Load Balancing (ELB). |  | D | T |  |  |  |
|  | 3.2.21.3 | (U) The system shall be able to support application auto-scaling. |  | D | T |  | I |  |
|  | 3.2.21.4 | (U) The system data capability shall be able to support elastic block storage volumes. |  |  | T |  |  |  |
| **3.3 (U) SWIF Application Requirements** | | | | | | | | |
| **3.3.1 (U//FOUO) Planning Application** | | | | | | | | |
|  | 3.3.1.1 | (U//FOUO) The system shall include a Planning application. |  | D |  |  |  |  |
|  | 3.3.1.2 | (U//FOUO) The system Planning application shall operate within the SWIF architecture. |  | D |  |  |  |  |
|  | 3.3.1.3 | (U//FOUO) The system Planning application shall use the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.4 | (U//FOUO) The system Planning application shall be capable of using the widgets within the SWIF Core Services. |  | D |  |  |  |  |
|  | 3.3.1.5 | (U//FOUO) The system shall include Planning widgets that allow users to perform CRUDA operations on Plans. |  | D |  |  |  |  |
|  | 3.3.1.6 | (U//FOUO) The system shall include Concept of Operations (CONOPS) widgets that allow users to perform CRUDA operations on CONOPS. |  | D |  |  |  |  |
|  | 3.3.1.7 | (U//FOUO) The system Planning application shall be capable of using the System and Common Services within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.8 | (U//FOUO) The system Planning Services shall be capable of using the Visualization Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.9 | (U//FOUO) The system Planning application shall be capable of using the User Account Management (UAM) Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.10 | (U//FOUO) The system Planning application shall be capable of using the Groups Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.11 | (U//FOUO) The system Planning application shall be capable of using the Search Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.12 | (U//FOUO) The system Planning application shall be capable of using the Workflow and Queues Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.13 | (U//FOUO) The system Planning application shall be capable of using the Import Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.14 | (U//FOUO) The system Planning application shall be capable of using the Export Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.15 | (U//FOUO) The system Planning application shall be capable of using the Named Area of Interest (NAI) Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.16 | (U//FOUO) The system Planning application shall be capable of using the Analytic Tools within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.17 | (U//FOUO) The system Planning application shall be capable of using the Production Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.18 | (U//FOUO) The system Planning application shall be capable of using the Notification Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.19 | (U//FOUO) The system Planning application shall be capable of using the Subscription Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.20 | (U//FOUO) The system Planning application shall be capable of using the Audit Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.21 | (U//FOUO) The system Planning application shall be capable of using the Usage and Performance Analytic Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.22 | (U//FOUO) The system Planning application shall be capable of using the System Configuration Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.23 | (U//FOUO) The system Planning application shall be capable of using the User Preference Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.24 | (U//FOUO) The system Planning application shall be capable of storing data in the system’s database. |  | D |  |  |  |  |
|  | 3.3.1.25 | (U//FOUO) The system Planning application shall comply with the UI requirements described within this document to provide a consistent user experience. |  | D |  |  |  |  |
|  | 3.3.1.26 | (U//FOUO) The system Planning application shall be capable of using the Help Service within the SWIF Common Services. |  | D |  |  |  |  |
|  | 3.3.1.27 | (U//FOUO) The system Planning Services shall provide the capability for a user to perform CRUDA operations on Plans. |  | D |  |  |  |  |
|  | 3.3.1.28 | (U//FOUO) The system Planning Services shall provide the capability for a user to perform CRUDA operations on Concepts of Operations (CONOPS). |  | D |  |  |  |  |
|  | 3.3.1.29 | (U//FOUO) The system Planning Services shall provide the capability for a user to perform CRUDA operations on Capabilities. |  | D |  |  |  |  |
|  | 3.3.1.30 | (U//FOUO) The system shall provide the capability for a user to set discretionary access (users or groups) to the Planning Services. |  | D |  |  |  |  |
|  | 3.3.1.31 | (U//FOUO) The system shall provide the capability for a user to develop a Concept of Operations (CONOP) for the selected capability specific to a Plan. |  | D |  |  |  |  |
|  | 3.3.1.32 | (U//FOUO) The system shall provide the capability for a user to display nodes and relationships. |  | D |  |  |  |  |
|  | 3.3.1.33 | (U//FOUO) The system shall provide the capability for a user to create a user-defined diagram of the overall Plan. |  | D |  |  |  |  |
|  | 3.3.1.34 | (U//FOUO) The system shall provide the capability for a user to create a product from a Plan. |  | D |  |  |  |  |
|  | 3.3.1.35 | (U//FOUO) The system shall provide the capability for a user to associate Capabilities to a Plan. |  | D |  |  |  |  |
|  | 3.3.1.36 | (U//FOUO) The system shall provide the capability for a user to associate Target Folders to a Plan. |  | D |  |  |  |  |
|  | 3.3.1.37 | (U//FOUO) The system shall provide the capability for a user to associate Target Folders and Capabilities to each other in support of creating a decision matrix. |  | D |  |  |  |  |
|  | 3.3.1.38 | (U//FOUO) The system shall provide the capability for a user to associate Plans to Concepts of Operations (CONOPS). |  | D |  |  |  |  |
|  | 3.3.1.39 | (U//FOUO) The system shall provide the capability for a user to create a user-defined capability of a specific Plan. |  | D |  |  |  |  |
|  | 3.3.1.40 | (U//FOUO) The system shall provide the capability for a user to create a SWIF Common Datta Model (CDM) Record. |  | D |  |  |  |  |
|  | 3.3.1.41 | (U//FOUO) The system shall provide the ability to link all created objects to a unique identifier associated with the SWIF user’s products. |  | D |  |  |  |  |
|  | 3.3.1.42 | (U//FOUO) The system shall provide the capability for a user to mark created items with the appropriate security markings. |  | D |  |  |  |  |
|  | 3.3.1.43 | (U//FOUO) The system shall provide the capability for a user to set discretionary access on previously created items. |  | D |  |  |  |  |
|  | 3.3.1.44 | (U//FOUO) The system shall provide the capability for a user to import Capabilities from an external source. |  | D |  |  |  |  |
|  | 3.3.1.45 | (U//FOUO) The system shall provide the capability for a user to import Target Folders from an external source. |  | D |  |  |  |  |
|  | 3.3.1.46 | (U//FOUO) The system shall provide the capability for a user to import other data for subsequent Planning analysis. |  | D |  |  |  |  |
|  | 3.3.1.47 | (U//FOUO) The system shall provide the capability for a user to use network diagrams. |  | D |  |  |  |  |
|  | 3.3.1.48 | (U//FOUO) The system shall provide problem definition tools. |  | D |  |  |  |  |
|  | 3.3.1.49 | (U//FOUO) The system shall provide decision support tools. |  | D |  |  |  |  |
|  | 3.3.1.50 | (U//FOUO) The system shall provide a course of action (COA) development support capability. |  | D |  |  |  |  |
|  | 3.3.1.51 | (U//FOUO) The system shall provide a simulation capability to assist in course of action (COA) development. |  | D |  |  |  |  |
| **3.3.2 (U) Target Folder Application** | | | | | | | | |
|  | 3.3.2.1 | (U) The system shall include a Target Folder application. |  | D |  |  |  |  |
|  | 3.3.2.2 | (U) The Target Folder application shall work with the SWIF core services. |  | D |  |  |  |  |
|  | 3.3.2.3 | (U) The system shall include a Target Folder widget that allows users to perform CRUDA operations on targets. |  | D |  |  |  |  |
|  | 3.3.2.4 | (U) The system shall provide the capability for the user to perform target feasibility analysis. |  | D |  |  |  |  |
| **3.4 (U) System Interface Requirements** | | | | | | | | |
| **3.4.1 (U) Interface Identification and Diagrams** | | | | | | | | |
| **3.4.2 (U) Internal Interfaces** | | | | | | | | |
|  | 3.4.2.1 | (U) The system’s hardware interfaces shall be compliant with referenced operations and computer/communications security requirements and standards. |  | D |  |  |  |  |
|  | 3.4.2.2 | (U) The system shall be capable of operating on Ethernet-based networks that support protocols including TCP/IP and HTTPS |  | D |  |  |  |  |
|  | 3.4.2.3 | (U) The system shall provide the capability to interface with a database. |  | D |  |  | I |  |
|  | 3.4.2.4 | (U) The system shall provide for secure connections (TLS) for all thick client communication. |  | D |  |  | I |  |
| **3.4.3 (U) External Interfaces** | | | | | | | | |
|  | 3.4.2.1 | (U) The configuration of the system’s controlled interface to the external systems shall be restricted to privileged Site Administrators. |  | D |  |  |  |  |
|  | 3.4.2.2 | (U) Data transmitted from an external systems controlled interface shall be audited. |  | D |  |  |  |  |
|  | 3.4.2.3 | (U) Data sent from external systems to the SWIF system shall include a classification marking for the classification of the content of the data exchange. |  | D |  |  |  |  |
|  | 3.4.2.4 | (U) The system shall provide for secure network connections (HTTPS) for all Web interfaces. |  | D | T |  |  |  |
|  | 3.4.2.5 | (U) The system shall provide the capability to interface with an external email server. |  | D |  |  |  |  |
|  | 3.4.2.6 | (U) The system shall provide a Web interface for all actions initiated by users. |  | D |  |  |  |  |
|  | 3.4.2.7 | (U) The system shall provide for a controlled interface with an image library. |  | D | T |  |  |  |
|  | 3.4.2.8 | (U) The system shall provide an OpenSearch interface to allow external systems to access SWIF data holdings. |  | D | T |  |  |  |
|  | 3.4.2.9 | (U) 3.4.3.9 The system shall provide a Web Processing Service (WPS) interface to allow external systems to access SWIF data holdings. |  | D |  |  |  |  |
|  | 3.4.2.10 | (U) The system shall provide a controlled interface with WMS/WFS-enabled servers. |  | D |  |  |  |  |
|  | 3.4.2.11 | (U) The system shall provide for a controlled interface with a map server. |  | D |  |  |  |  |
|  | 3.4.2.12 | (U) The system shall provide a capability for managing taskings to external systems. |  | D |  |  |  |  |
|  | 3.4.2.13 | (U) The system shall provide a controlled interface with requirements management systems. |  | D |  |  |  |  |
|  | 3.4.2.14 | (U) The system shall provide a controlled interface with external analytic systems. |  | D |  |  |  |  |
|  | 3.4.2.15 | (U) The system shall provide the capability to monitor communications between the SWIF system and external systems. |  | D |  |  |  |  |
|  | 3.4.2.16 | (U) The system shall provide a controlled interface with the Modernized Integrated Data Bases (MIDB). |  | D |  |  |  |  |
|  | 3.4.2.17 | (U) The system shall provide the capability to export SWIF documents into a SWIF-defined format. |  | D |  |  |  |  |
| **3.5 (U) System Internal Data Requirements** | | | | | | | | |
| **3.6 (U) Adaptation Requirements** | | | | | | | | |
|  | 3.6.1. | (U) A test/training system shall be made available. |  | D |  |  |  |  |
|  | 3.6.2 | (U) The test/training system shall have, as a minimum, the same functionality as the operational system. |  | D |  |  |  |  |
|  | 3.6.3 | (U) A variant of the system shall be made available to support a Coalition environment. |  | D |  |  |  |  |
| **3.7 (U) Safety Requirements** | | | | | | | | |
|  | 3.7.1 | (U) The system shall comply with best safety practices to minimize potential hazards. |  |  | I |  |  |  |
|  | 3.7.2 | (U) Warnings shall be issued to users before system shutdown. |  | D |  |  |  |  |
| **3.8 (U) Security Requirements** | | | | | | | | |
| **3.8.1 (U) Security** | | | | | | | | |
|  | 3.8.1.1 | (U) The system shall comply with Intelligence Community Directives on security controls on the dissemination of intelligence information. |  | D |  |  |  |  |
|  | 3.8.1.2 | (U) The system shall meet collateral Department of Defense security certification/accreditation requirements. |  | D |  |  |  |  |
|  | 3.8.1.3 | (U) The system shall meet Intelligence Community Sensitive Compartmented Information (SCI) security certification/accreditation requirements, as applicable. |  | D |  |  |  |  |
|  | 3.8.1.4 | (U) The system shall be accessible only to authorized users. |  | D |  |  |  |  |
|  | 3.8.1.5 | (U) The system shall require a user to log on to the system before the user can access the system application and its resources for any functionality other than viewing or creating items at the unclassified level. |  | D |  |  |  |  |
|  | 3.8.1.6 | (U) The system shall allow for a visitor account. |  | D |  |  |  |  |
|  | 3.8.1.7 | (U) The system shall allow for only a single session per user account (with the exception of the guest/visitor account). |  | D |  |  |  |  |
|  | 3.8.1.8 | (U) The system shall include an Identification and Authentication (I&A) management mechanism that uniquely identifies and authenticates. |  | D |  |  |  |  |
|  | 3.8.1.9 | (U) The system shall provide for secure user login authentication and authorization for system access. |  | D |  |  |  |  |
|  | 3.8.1.10 | (U) The system shall include read-only classification banners within each user interface (UI) screen displayed. |  | D |  |  |  |  |
|  | 3.8.1.11 | (U) The system shall display classification banners within each system window being displayed with a background color matching the appropriate classification level. |  | D |  |  |  |  |
|  | 3.8.1.12 | (U) The system shall allow the Site Administrator to set the classification instructions in the banner displayed to the system user. |  | D |  |  |  |  |
|  | 3.8.1.13 | (U) All factory (including commercial) default passwords for the system shall be changed before operational deployment. |  | D |  |  | I |  |
|  | 3.8.1.14 | (U) The system shall ensure system notifications are destined for the correct recipient, based on the type of notification. |  | D |  | A |  |  |
|  | 3.8.1.15 | (U) The system shall ensure the content of a notification for the intended recipient is appropriate for the type of notification. |  | D |  |  |  |  |
|  | 3.8.1.16 | (U) The system shall validate the integrity information associated with each notification. |  | D |  |  |  |  |
|  | 3.8.1.17 | (U) The system shall provide the ability to monitor notifications transmitted from the system to external systems. |  | D |  |  |  |  |
|  | 3.8.1.18 | (U) The system shall provide a role-based access control system to support a single log-on capability based on an individual user profile. |  | D |  |  |  |  |
|  | 3.8.1.19 | (U) The system shall authenticate each user using strong authentication mechanisms over secure channels before authorizing access to the system. |  | D |  |  |  |  |
|  | 3.8.1.20 | (U) The system shall only use Transport Layer Security (TLS) encryption mechanisms that are Federal Information Processing Standards (FIPS) 140-2 compliant. |  |  |  |  | I |  |
|  | 3.8.1.21 | (U) The system shall provide the capability for a user to hide information from view by other users as a feature to support need-to-know (NTK) access. |  | D |  |  |  |  |
|  | 3.8.1.22 | (U) The system shall protect all identified data items. |  | D |  |  |  |  |
|  | 3.8.1.23 | (U) The system shall restrict read access to data based on Controlled Access Program Coordination Office (CAPCO) guidelines (including classification). |  | D |  |  |  |  |
|  | 3.8.1.24 | (U) The system shall restrict access to actions based on roles with associated privileges. |  | D |  |  |  |  |
|  | 3.8.1.25 | (U) The system shall support the ability of a user to be able to hide his account from appearing in objects associated with system. |  | D |  |  |  |  |
|  | 3.8.1.26 | (U) The system shall support the ability of a user to be able to associate an alias with the user’s account. |  | D |  |  |  |  |
|  | 3.8.1.27 | (U) The system shall be able to associate external user authentication information to a SWIF Role. |  | D |  |  |  |  |
|  | 3.8.1.28 | (U) The system shall enforce password complexity in compliance with the targeted deployment network. |  | D |  |  |  |  |
|  | 3.8.1.29 | (U) The system shall establish a trusted path to each user. |  | D |  |  |  |  |
|  | 3.8.1.30 | (U) Upon successful identification and authentication, the system shall establish a protected path between each authorized user and the system. |  | D |  | A |  |  |
|  | 3.8.1.31 | (U) The system shall provide a mechanism that will prevent unauthorized use of security-relevant system functions including related data. |  | D | T |  |  |  |
|  | 3.8.1.32 | (U) The system shall provide a mechanism that will detect unauthorized use of security-relevant system functions including related data. |  | D | T |  |  |  |
|  | 3.8.1.33 | (U) The system shall generate an audit record for unauthorized attempts to use security-relevant functions including related data. |  | D |  |  |  |  |
|  | 3.8.1.34 | (U) The system shall provide a mechanism that will prevent the unauthorized modification of security-relevant functions including related data. |  | D | T |  |  |  |
|  | 3.8.1.35 | (U) The system shall provide a mechanism to detect unauthorized modification of security-relevant functions including related data. |  | D | T |  |  |  |
|  | 3.8.1.36 | (U) The system shall generate an audit record for unauthorized attempts to modify security-relevant functions including related data. |  | D | T |  |  |  |
|  | 3.8.1.37 | (U) The system shall provide a mechanism that will enforce the “Principle of Least Privilege” on security-relevant functions. |  | D |  |  |  |  |
|  | 3.8.1.38 | (U) The system shall prevent interference with its operation by removing all residual data generated during its processing when that processing is concluded. |  | D |  |  | I |  |
|  | 3.8.1.39 | (U) The system shall prevent access to information previously contained in objects that have been unallocated. |  | D |  |  | I |  |
|  | 3.8.1.40 | (U) The system shall provide a mechanism that will prevent the bypass of security functions. |  | D |  |  | I |  |
|  | 3.8.1.41 | (U) The system shall provide a mechanism to search specified objects for malicious content defined by the malicious content profile(s). |  | D |  |  | I |  |
|  | 3.8.1.42 | (U) If malicious content is found, the system shall generate an audit record and perform other actions specified by the requestor. |  | D |  |  |  |  |
|  | 3.8.1.43 | (U) The audit record for the malicious content detection shall support evaluating the detected content. |  | D |  |  |  |  |
|  | 3.8.1.44 | (U) The system shall assign restrictive default values for the access control attributes of all subjects and objects when they are created. |  | D |  |  | I |  |
|  | 3.8.1.45 | (U) The system shall assign the MAC attributes to the access control attributes for all subjects and objects residing on systems enforcing a MAC policy. |  | D |  |  | I |  |
|  | 3.8.1.46 | (U) The system shall provide the capability for a subject to obtain the DAC attributes (e.g., group membership or access type) for a particular subject (user) or object they dominate. |  | D |  |  | I |  |
|  | 3.8.1.47 | (U) The system shall provide the ability for a subject residing on systems enforcing a MAC policy to obtain the MAC attribute values of a subject or object they dominate. |  | D |  |  | I |  |
|  | 3.8.1.48 | (U) The system shall provide the ability for a subject to determine whether it has DAC access to a named object. |  | D |  |  | I |  |
|  | 3.8.1.49 | (U) The system shall be able to compare two sets of MAC attribute values to determine their dominance relationship. |  | D |  |  | I |  |
|  | 3.8.1.50 | (U) The system shall be able to determine whether the values for the MAC attributes assigned to a subject or object are valid, to include conforming to the relationship rules for MAC attributes. |  | D |  |  | I |  |
|  | 3.8.1.51 | (U) The system shall mediate access to an object by a subject, based on the access control attributes and policies extant on a given component. |  | D |  |  | I |  |
|  | *[3.8.1.52* | *(U) not used; added to 3.2.13.1]* | *N/A* |  |  |  |  |  |
|  | 3.8.1.53 | (U) The system shall provide a service to generate non-repudiation data. |  | D |  |  | I |  |
|  | 3.8.1.54 | (U) The system shall generate a non-repudiation record whenever the system generates non-repudiation data. |  | D |  |  |  |  |
|  | 3.8.1.55 | (U) The system shall provide a service to verify the authenticity of non-repudiation data. |  | D |  |  |  |  |
|  | 3.8.1.56 | (U) The system shall generate a non-repudiation record whenever the system validates non-repudiation data. |  | D |  |  | I |  |
|  | 3.8.1.57 | (U) The system shall generate a non-repudiation record when the system verifies the authenticity of non-repudiation data. |  | D |  |  |  |  |
|  | 3.8.1.58 | (U) The system shall provide the capability for the ISSO to retrieve non-repudiation records. |  | D |  |  |  |  |
|  | 3.8.1.59 | (U) The system shall preserve non-repudiation records for forensic analysis. |  | D |  |  |  |  |
|  | 3.8.1.60 | (U) The system shall generate audit records capturing security-relevant events. |  | D |  |  |  |  |
|  | 3.8.1.61 | (U) The system shall store generated audit events into an audit log that is protected against unauthorized modification. |  | D |  |  |  |  |
|  | 3.8.1.62 | (U) The audit log shall be capable of being exported by authorized privileged users. |  | D |  |  |  |  |
|  | 3.8.1.63 | (U) The system shall provide the capability for the ISSO to obtain an audit record. |  | D |  |  |  |  |
|  | 3.8.1.64 | (U) The system shall be able to perform a backup operation. |  | D |  |  |  |  |
|  | 3.8.1.65 | (U) The system shall be able to perform a restore operation. |  | D |  |  |  |  |
|  | 3.8.1.66 | (U) The system shall be able to perform a backup of security-relevant functions including data on request. |  | D |  |  |  |  |
|  | 3.8.1.67 | (U) The system shall be able to restore, on request, the security-relevant functions including data up to the last backup archive. |  | D |  |  |  |  |
|  | 3.8.1.68 | (U) The systems shall be capable of being restored to the last known secure configuration through the application of the recorded changes to security-relevant data including functions. |  | D |  |  |  |  |
|  | 3.8.1.69 | (U) The system shall provide the capability to generate an integrity seal for data that permits modification of the original data to be detected. |  | D |  |  | I |  |
|  | 3.8.1.70 | (U) The system shall provide the capability to validate the integrity seal that has been generated for data. |  | D |  |  | I |  |
|  | 3.8.1.71 | (U) The system shall provide the capability to ensure the confidentiality of data through encryption. |  | D |  |  | I |  |
|  | 3.8.1.72 | (U) The system shall provide the capability to decrypt encrypted data. |  | D |  |  |  |  |
|  | 3.8.1.73 | (U) The system shall require all users interacting with the system to identify themselves to include authenticating their claimed identity. |  | D |  |  |  |  |
|  | 3.8.1.74 | (U) The system shall notify users that their authenticator will expire within an ISSO-specified period prior to the authenticator’s expiration. |  | D |  |  |  |  |
|  | 3.8.1.75 | (U) The system shall make an authenticator unusable after an ISSO-specified lifetime. |  | D |  |  |  |  |
|  | 3.8.1.76 | (U) The system shall be able to obtain identification and authentication attributes (e.g., user ID) for a user from the user profile identification and authentication attributes. |  | D |  |  |  |  |
|  | 3.8.1.77 | (U) The system shall invoke the appropriate user interface based on user authentication. |  | D |  |  |  |  |
|  | 3.8.1.78 | (U) The system shall provide the capability for an individual authorized user to update the user’s own user identification and authentication attributes maintained in the user profile. |  | D |  |  |  |  |
|  | 3.8.1.79 | (U) The system shall ensure that user passwords are sufficiently strong for reliable authentication by conforming with FIPS 181, Automated Password Generator (APG), October 1993. |  | D |  |  | I |  |
|  | 3.8.1.80 | (U) The system shall provide a reliable time source to its components. |  | D |  |  |  |  |
|  | *[3.8.1.81* | *(U) not used; added to 3.2.13.1]* | *N/A* |  |  |  | I |  |
|  | 3.8.1.82 | (U) The system shall provide the capability to adjust the reliable time source with values obtained from an authorized reference time source. |  | D |  |  |  |  |
| **3.8.2 (U) Privacy** | | | | | | | | |
|  | 3.8.2.1 | (U) The system shall comply with the provisions of the Foreign Intelligence Surveillance Act as it pertains to the collection and retention of data on U.S. persons. |  | D |  |  | I |  |
|  | 3.8.2.2 | (U) The system shall provide the capability to notify the Site Administrator automatically when information held about a U.S. Person is reaching its expiration date. |  | D |  |  |  |  |
|  | 3.8.2.3 | (U) The system shall comply with the Privacy Act of 1974. |  | D |  |  | I |  |
| **3.9 (U) System Environment Requirements** | | | | | | | | |
|  | 3.9.1 | (U) The system shall operate in a commercial computer environment using commercial electrical power. |  | D |  |  | I |  |
|  | 3.9.2 | (U) The system shall not impose any environmental constraints on the host hardware system. |  | D |  |  |  |  |
| **3.10 (U) Computer Resource Requirements** | | | | | | | | |
| **3.10.1 (U) Computer Hardware** | | | | | | | | |
|  | 3.10.1.1 | (U) The system shall be capable of having the servers deployed on different host machines. |  | D |  |  |  |  |
|  | 3.10.1.2 | (U) If deployed on multiple host machines, the system shall be deployed on a server which meets the current system capabilities. |  | D |  |  |  |  |
|  | 3.10.1.3 | (U) The system shall be capable of being deployed with the servers on the same host machine. |  | D |  |  |  |  |
|  | 3.10.1.4 | (U) If deployed on a single host machine, the system shall be deployed on a server which meets the current system minimum capabilities. |  | D |  |  |  |  |
| **3.10.2 (U) Computer Hardware Resource Utilization Requirements** | | | | | | | | |
| **3.10.3 (U) Computer Software Requirements** | | | | | | | | |
|  | 3.10.3.1 | (U) The system shall operate, as a minimum, on two servers. |  | D |  |  |  |  |
|  | 3.10.3.2 | (U) The system server shall support cross-platform deployment. |  | D |  |  |  |  |
|  | 3.10.3.3 | (U) The system shall support multiple browsers. |  | D |  |  |  |  |
|  | 3.10.3.4 | (U) The system shall deny access by users who attempt to access the system using a Web browser that has not been approved by the target network Chief Information Officer (CIO). |  | D |  |  |  |  |
| **3.10.4 (U) Computer Communications Requirements** | | | | | | | | |
|  | 3.10.4.1 | (U) The system shall use mechanisms to prevent the hijacking of a communications session. |  | D |  |  |  |  |
|  | 3.10.4.2 | (U) The system shall use Special Purpose Network systems with associated networks accredited to handle classified information. | N/A |  |  |  |  |  |
|  | 3.10.4.3 | (U) The system’s latency shall not exceed 5 seconds to respond to a service request. |  | D |  |  |  |  |
|  | 3.10.4.4 | (U) The system shall support data ingest of at least 1000 messages in an hour. |  | D |  |  |  |  |
|  | 3.10.4.5 | (U) The system shall support 50 concurrent users per site installation. |  | D |  |  |  |  |
|  | 3.10.4.6 | (U) The system shall provide error messages for failed transmissions. |  | D |  |  |  |  |
|  | 3.10.4.7 | (U) The systems shall provide the capability to generate and display metrics. |  | D |  |  |  |  |
| **3.11 (U) System Quality Factors** | | | | | | | | |
| **3.11.1 (U) Functionality** | | | | | | | | |
| **3.11.2 (U) Performance** | | | | | | | | |
|  | 3.11.2.1 | (U) The average response time for a system transaction must not exceed five (5) seconds. |  | D | T |  |  |  |
|  | 3.11.2.2 | (U) The maximum response time for a system transaction must not exceed ten (10) seconds. |  | D | T |  |  |  |
|  | 3.11.2.3 | (U) The system must be capable of handling X transactions per second during normal operations. |  | D | T |  |  |  |
|  | 3.11.2.4 | (U) The system must be capable of handling X transactions per second during emergency operations. |  | D | T |  |  |  |
|  | 3.11.2.5 | (U) The system must be capable of supporting X number of simultaneous users during peacetime mode. |  | D | T |  |  |  |
|  | 3.11.2.6 | (U) The system must be capable of supporting X number of simultaneous users during wartime mode. |  | D | T |  |  |  |
|  | 3.11.2.7 | (U) The system must be capable of operating in a degraded mode. |  | D | T |  |  |  |
|  | 3.11.2.8 | (U) Resource utilization (memory, disk, communications). |  | D | T |  |  |  |
|  | 3.11.2.9 | (U) The system must verify user login information within five (5) seconds. |  | D | T |  |  |  |
|  | 3.11.2.10 | (U) Queries must return results within five (5) seconds. |  | D | T |  |  |  |
|  | 3.11.2.11 | (U) System functions must be initiated within 500 μsecs after their selection. |  | D | T |  |  |  |
|  | 3.11.2.12 | (U) User-selected pages must be displayed within five (5) seconds after their selection. |  | D | T |  |  |  |
| **3.11.3 (U) Reliability** | | | | | | | | |
|  | 3.11.3.1 | (U) Failure of a given system component shall not precipitate a failure in its backup equipment. |  |  | T |  |  |  |
|  | 3.11.3.2 | (U) Failure of the system’s software components shall not cause failures in interfacing components. |  |  | T |  |  |  |
|  | 3.11.3.3 | (U) The system shall achieve a mean time between critical failures (MTBCF) of at least 5,000 hours. |  |  | T |  |  |  |
| **3.11.4 (U) Maintainability** | | | | | | | | |
|  | 3.11.4.1 | (U) The system shall have a Mean Corrective Maintenance Time (MCMT) of no greater than one hour and a Mean Maximum Corrective Time (MMCT) of 2 hours (90th percentile). |  |  | T |  |  |  |
|  | 3.11.4.2 | (U) The system shall mark audit table entries with severity (level) values to assist in isolating defects for their cause. |  | D |  |  |  |  |
|  | 3.11.4.3 | (U) To reduce the mean time to repair, the system shall minimize the use of “hard-coding” values. |  |  |  |  | I |  |
|  | 3.11.4.4 | (U) The system shall be developed in the Java software language to improve maintainability. |  |  |  |  | I |  |
|  | 3.11.4.5 | (U) The system shall be implemented in a layered architecture. |  |  |  |  | I |  |
|  | 3.11. 4.6 | (U) The system shall be implemented to be modular. |  |  |  |  | I |  |
|  | 3.11.4.7 | (U) The system shall be implemented to maximize encapsulation to hide the values or state of a structured data object inside a class, preventing unauthorized parties direct access to them. |  |  |  |  | I |  |
|  | 3.11.4.8 | (U) The system shall be implemented with well-defined interfaces. |  |  |  |  | I |  |
|  | 3.11.4.9 | (U) The system shall be implemented using object-orientation and component-based development. |  |  |  |  | I |  |
|  | *[3.11.4.10* | *(U) Not used pending refinement of statement.]* | *N/A* |  |  |  |  |  |
|  | 3.11.4.11 | (U) The system design shall be documented in the form of Software Design Descriptions for each component. |  |  |  |  | I |  |
|  | 3.11.4.12 | (U) The system’s interface design shall be documented in the form of Interface Design Descriptions for each interface defined by the system for use by external systems. |  |  |  |  | I |  |
|  | 3.11.4.13 | (U) The system’s interface design shall be documented in the form of an Interface Control Document for all of the system’s interfaces. |  |  |  |  | I |  |
|  | 3.11.4.14 | (U) The system’s software code shall contain comments by the developer to support maintainability. |  |  |  |  | I |  |
|  | 3.11.4.15 | (U) The system shall be designed and implemented with adherence to project conventions. |  |  |  |  | I |  |
|  | 3.11.4.16 | (U) The average person-time required to fix a Priority 3 defect shall not exceed two person-days. | N/A |  |  |  |  |  |
|  | 3.11.4.17 | (U) The average person-time required to fix a Priority 2 defect shall not exceed one person-week. | N/A |  |  |  |  |  |
|  | 3.11.4.18 | (U) The average person-time required to make a minor enhancement shall not exceed one person-week. | N/A |  |  |  |  |  |
|  | 3.11.4.19 | (U) Dead code shall not be retained in the system. |  |  |  |  | I |  |
|  | 3.11.4.20 | (U) Redundant code shall not be retained in the system. |  |  |  |  | I |  |
|  | 3.11.4.21 | (U) The system shall be designed with enough flexibility to support new protocols as they emerge without requiring a software redesign. | N/A |  |  |  |  |  |
| **3.11.5 (U) Availability** [Note: some requirement statements in this subsection are still under development (as indicated by “X” placeholders.] | | | | | | | | |
|  | 3.11.5.1 | (U) The MTBF for Critical failures shall be X weeks, averaged over X months. |  |  | T |  |  |  |
|  | 3.11.5.2 | (U) The minimum time between Critical failures shall be in excess of X days. |  |  | T |  |  |  |
|  | 3.11.5.3 | (U) The MTBF for Warning failures shall be X weeks, averaged over X months. |  |  | T |  |  |  |
|  | 3.11.5.4 | (U) The minimum time between Warning failures shall be in excess of X days. |  |  | T |  |  |  |
|  | 3.11.5.5 | (U) The system shall not have more than five (5) hours of scheduled downtime per month. |  |  | T |  |  |  |
|  | 3.11.5.6 | (U) The system shall not more than an average of one (1) hour of unscheduled downtime per month. |  |  | T |  |  |  |
|  | 3.11.5.7 | (U) The MTTR for the system shall not exceed X hours after it has failed. |  |  | T |  |  |  |
|  | 3.11.5.8 | (U) Administrative reporting shall have an availability of 98%. |  |  | T |  |  |  |
|  | 3.11.5.9 | (U) All Planning functionality has a planned availability of 24 hours per day, 365 days per year. |  |  | T |  |  |  |
|  | 3.11.5.10 | (U) User access to persistent data shall have an availability of 99.999%. |  |  | T |  |  |  |
|  | 3.11.5.11 | (U) At least one data center shall be available at all times at least 99.999% of the time. |  |  | T |  |  |  |
|  | 3.11.5.12 | (U) The SWIF system will not provide functionality for capturing memory usage. |  | D |  |  |  |  |
|  | 3.11.5.13 | (U) The system shall provide the ability to perform remote maintenance per the host site System Security Authorization Agreement (SSAA). |  | D |  |  |  |  |
|  | 3.11.5.14 | (U) SWIF availability requirements shall be determined by the Project Manager using Information Assurance (IA) Implementation guidance. |  |  | T |  |  |  |
| **3.11.6 (U) Portability** | | | | | | | | |
|  | 3.11.6.1 | (U) The system software shall be capable of being re-hosted to more powerful processing platforms in support of an expanded user capacity. |  | D |  |  |  |  |
|  | 3.11.6.2 | (U) The system shall be capable of running on a Linux operating system. |  | D |  |  |  |  |
|  | 3.11.6.3 | (U) The system shall be capable of running on a Mac operating system. |  | D |  |  |  |  |
|  | 3.11.6.4 | (U) The system shall be capable of running on a Fedora operating system. |  | D |  |  |  |  |
|  | 3.11.6.5 | (U) Porting the application from Linux OS to Windows OS shall not require more than 24 person weeks in time. |  |  | T |  |  |  |
|  | 3.11.6.6 | (U) The average time needed to port the application to Internet Explorer shall not exceed 12 person weeks. |  |  | T |  |  |  |
|  | 3.11.6.7 | (U) The system shall improve portability by isolating operating system calls. |  |  |  | I |  |  |
|  | 3.11.6.8 | (U) The system shall minimize the use of machine language. |  |  |  | I |  |  |
|  | 3.11.6.9 | (U) The system shall be written in Java to maximize portability. |  |  |  | I |  |  |
|  | 3.11.6.10 | (U) The system shall use open interface standards to maximize portability. |  |  |  | I |  |  |
|  | 3.11.6.11 | (U) The system shall maximize the use of open interface standards. |  |  |  | I |  |  |
| **3.11.7 (U) Reusability** | | | | | | | | |
|  | 3.11.7.1 | (U) Reusability shall be considered in the design of SWIF. | N/A |  |  |  |  |  |
|  | 3.11.7.2 | (U) The architecture of service components for SWIF shall consider existing APIs. |  | D | T |  | I |  |
|  | 3.11.7.3 | (U) A minimum of 30% of the application’s software shall be potentially reusable on future endeavors. | N/A |  |  |  |  |  |
| **3.11.8 (U) Testability** | | | | | | | | |
|  | 3.11.8.1 | (U) The system shall be compliant with the requirements specified by the Joint Interoperability Test Command (JITC). |  | D |  |  |  |  |
|  | 3.11.8.2 | (U) Only testers shall test system software. |  | D |  |  |  |  |
|  | 3.11.8.3 | (U) The system shall provide a test interface that enables its state to be observed. |  | D |  |  |  |  |
|  | 3.11.8.4 | (U) For defined interfaces with external systems, the system shall be delivered with associated test software including test data that is sufficient to enable testing between the system and the external system. |  | D | T |  |  |  |
|  | 3.11.8.5 | (U) The system shall provide a human interface that enables the user with the Tester role to perform system testing tasks. |  | D |  |  |  |  |
|  | 3.11.8.6 | (U) The system shall include built-in self-test software that automatically tests the system while it is in operation. |  | D | T |  |  |  |
| **3.11.9 (U) Usability** | | | | | | | | |
|  | 3.11.9.1 | (U) The system shall evoke in its users the feeling that its output is credible. |  | D |  |  |  |  |
|  | 3.11.9.2 | (U) The system shall not require its users to perform numerous steps before they can begin using it. |  | D |  |  |  |  |
|  | 3.11.9.3 | (U) The system shall be easy for its users to remember how to use. |  | D |  |  |  |  |
|  | 3.11.9.4 | (U) The system’s user interface shall not require the user to either remember or copy information from one screen/webpage to another. |  | D |  |  |  |  |
|  | 3.11.9.5 | (U) The system help functionality shall be easy to locate. |  | D |  |  |  |  |
|  | 3.11.9.6 | (U) The system shall be easy for its users to use. |  | D |  |  |  |  |
|  | 3.11.9.7 | (U) The system shall be 508 compliant. |  | D |  |  |  |  |
|  | 3.11.9.8 | (U) The system shall improve the effectiveness of its users. |  | D |  |  |  |  |
|  | 3.11.9.9 | (U) The system shall minimize the errors made by its users. |  | D |  |  |  |  |
|  | 3.11.9.10 | (U) The system shall minimize the errors made by its users by performing field validation to the maximum extent possible. |  | D |  |  |  |  |
|  | 3.11.9.11 | (U) The system’s user interface shall make it easy for users to navigate to where they want to go. |  | D |  |  |  |  |
|  | 3.11.9.12 | (U) Users of the system shall be able to navigate to major functions in one click from the main menu bar. |  | D |  |  |  |  |
|  | 3.11.9.13 | (U) The system shall enable users to retrieve data in the form they want. |  | D |  |  |  |  |
|  | 3.11.9.14 | (U) The system shall enable users to download work product in the formats they need. |  | D |  |  |  |  |
|  | 3.11.9.15 | (U) The system shall be suitable for experienced users to use. |  | D |  |  |  |  |
|  | 3.11.9.16 | (U) The system shall be suitable for novice users to use. |  | D |  |  |  |  |
|  | 3.11.9.17 | (U) The system’s user interface shall be clear to its users. |  | D |  |  |  |  |
|  | 3.11.9.18 | (U) The system’s help facilities shall be unambiguous to the users. |  | D |  |  |  |  |
|  | 3.11.9.19 | (U) The system’s user-oriented error messages shall be easy for its users to understand. |  | D |  |  |  |  |
|  | 3.11.9.20 | (U) The system’s user guide shall be organized logically. |  | D |  |  | I |  |
|  | 3.11.9.21 | (U) The system’s installation and system administration guide shall be organized logically. |  | D |  |  | I |  |
|  | 3.11.9.22 | (U) The system shall be beneficial to its users. |  | D |  |  |  |  |
| **3.12 (U) Design and Construction Constraints** | | | | | | | | |
|  | 3.12.1 | (U) The system shall only provide email notification services if the host environment provides access to an email server for the system to use. |  | D |  |  |  |  |
|  | 3.12.2 | (U) The system design shall incorporate technology insertion concepts such that software components and hardware platforms can be modularly upgraded over time to take advantage of state-of-the-art technical advances in commercial information technology. | N/A |  |  |  |  |  |
|  | *[3.12.3* | *(U) Not used pending refinement of statement.]* | *N/A* |  |  |  |  |  |
|  | 3.12.4 | (U) The system shall be developed in Java to meet quality factors. |  |  |  |  | I |  |
|  | 3.12.5 | (U) The system shall be capable of operating within the OZONE Widget Framework OWF environment. |  | D |  |  | I |  |
|  | 3.12.6 | (U) The system shall be capable of operating within the Intelligence Community Information Technology Enterprise (ICITE). |  | D |  |  |  |  |
| **3.13 (U) Personnel-Related Requirements** | | | | | | | | |
|  | 3.13.1 | (U) The systems users shall have experience in using browser-based applications. | N/A |  |  |  |  |  |
|  | 3.13.2 | (U) The system Administrative users shall have technical experience that exceeds the level of an average user. | N/A |  |  |  |  |  |
| **3.14 (U) Training-Related Requirements** | | | | | | | | |
|  | 3.14.1 | (U) The system users shall be trained initially via on-site training. | N/A |  |  |  |  |  |
|  | 3.14.2 | (U) Follow-on training for the system shall be via multiple avenues. | N/A |  |  |  |  |  |
|  | 3.14.3 | (U) The system shall not require users to take significant training to learn to use it to perform their tasks. |  | D |  |  |  |  |
|  | 3.14.4 | (U) Training materials for the system shall include multiple products. |  |  |  |  | I |  |
|  | 3.14.5 | (U) The SWIF system training material shall be available via multiple means |  |  |  |  | I |  |
| **3.15 (U) Logistic-Related Requirements** | | | | | | | | |
|  | 3.15.1 | (U) A Government-Contractor Integrated Product Team (IPT) shall deliver instructions detailing the procedures required for the use of any Commercial-off-the-Shelf (COTS) required by the SWIF system. |  |  |  |  | I |  |
|  | 3.15.2 | (U) A Government-Contractor Integrated Product Team (IPT) shall deliver instructions detailing the procedures required for the use of any Government-off-the-Shelf (GOTS) required by the SWIF system. |  |  |  |  | I |  |
|  | 3.15.3 | (U) A Government-Contractor Integrated Product Team (IPT) shall deliver listings of all required materials. |  |  |  |  | I |  |
|  | 3.15.4 | (U) A Government-Contractor Integrated Product Team (IPT) shall provide SWIF system maintenance. | N/A |  |  |  |  |  |
|  | 3.15.5 | (U) A Government-Contractor Integrated Product Team (IPT) shall provide software support for the SWIF system. | N/A |  |  |  |  |  |
|  | 3.15.6 | (U) The SWIF system shall generate reports showing information about the maintenance schedule. |  | D |  |  |  |  |
|  | *[3.15.7* | *(U) not used; added to 3.2.13.1]* | N/A |  |  |  |  |  |
|  | 3.15.8 | (U) The system shall be implemented to allow Administrators to conduct remote administration. |  | D |  |  |  |  |
|  | 3.15.9 | (U) The deployment of the system shall not affect existing facilities already established to support special programs. |  | D |  |  |  |  |
|  | 3.15.10 | (U) The deployment of the system shall require dedicated equipment. | N/A |  |  |  |  |  |
|  | 3.15.11 | (U) The system shall xxx to prevent accidental destruction of the software. |  | D |  |  |  |  |
|  | 3.15.12 | (U) The system shall xxx to prevent accidental loss of data. |  | D |  |  |  |  |
| **3.16 (U) Other Requirements** | | | | | | | | |
| **3.17 (U) Packaging and Labeling Requirements** | | | | | | | | |
|  | 3.17.1 | (U) The SWIF system shall be made available for third-party use using means determined by the SWIF Project Manager and the target network Security Manager. |  |  |  |  | I |  |
|  | 3.17.2 | (U) All physical media shall be properly marked. |  |  |  |  | I |  |
| **3.18 (U) Precedence And Criticality Of Requirements** | | | | | | | | |

# (U) REQUIREMENTS TRACEABILITY

(U) This section is tailored out; per the SSS Data Item Description, this section does not apply to system specifications.

# (U) PRECURSOR OF SWIF BASELINE REQUIREMENTS

The SSC Pacific SWIF Team Lead, requested SAIC identify the SWIF baseline requirements from the SWIF enterprise requirements documented in the June 26, 2013, version of the System, Sub-System Specification (SSS) Guide.

SAIC did not participate in the development of the original SWIF requirements, however, authored the SSS and identified requirements at the enterprise level in the event SWIF matures to a Program of Record. These enterprise requirements were the basis to estimate the current baseline SWIF requirements.

On Monday, July 22, 2013, the SSC Pacific SWIF Team Lead and the SCC Pacific SWIF System Engineer met with the SAIC to verify the estimated baseline requirements and clarify questionable requirements.

The following requirements are a subset of the enterprise requirements identified in Section 3 and were verified by the SWIF Team as the SWIF baseline requirements. The Section 3 numbering schema remains intact to trace the requirements to a particular sub-section.

**Section 3.2 (U) SWIF Core Service Requirements:**

**Section 3.2.1 (U) System and Common Utilities:**

**(U) 3.2.1.1 The system shall provide access using existing communications architectures.**

(U) These architectures may include a variety of existing wired or wireless networks and broadcasts.

**(U) 3.2.1.2 The SWIF software shall support existing networks that implement the TCP/IP communication protocol.**

**(U) 3.2.1.4 Each system-generated entity shall have a unique identifier.**

(U) This unique identifier can support traceability and linkage.

**(U) 3.2.1.6 The system shall be able to authenticate user access using external authentication servers.**

(U) This authentication will use the protocols (e.g., Defense Contract Action Data System, DCADS; Active Directory, AD; Open Directory; Lightweight Directory Access Protocol, LDAP) associated with the external authentication servers.

**(U) 3.2.1.7 The system shall comply with the ICD 503 security requirements directed by the DAA.**

(U) ICD 503 defines security requirements for the assigned Protection Level and Levels of Concern for Availability and Integrity.

**(U) 3.2.1.10 The system shall provide a security service to control access to the system.**

(U) System access control includes providing user authentication and authorization.

**(U) 3.2.1.11 The system shall control access to system functionality based on the user’s role.**

(U)This includes role-based access control (RBAC).

**(U) 3.2.1.12 The system shall control access to system data based on the user’s attributes including clearance.**

(U) The system uses the clearance data to determine row- and cell-based security.

**(U) 3.2.1.13 The system shall implement security features commensurate with Protection Level (PL) 3 identified for the system interfaces for the deployed network.**

**(U) 3.2.1.18 The system shall provide for visualization capabilities.**

(U) Required visualization capabilities include those which allow users to display the data stored within the system.

**(U) 3.2.1.19 The system shall provide users a customizable display composed of widgets for interacting with data in the data store.**

(U) These widgets will support viewing and manipulating data in the data store.

**(U) 3.2.1.21 The system shall provide users the capability to set Discretionary Access to information stored in the system.**

(U) This Discretionary Access can be Group or Individual(s).

**Section 3.2.2 (U) Visualization**

**(U) 3.2.2.1 The system shall include a user interface (UI) experience that includes widgets for general user functionality.**

**(U) 3.2.2.2 The system shall allow the user to configure widgets into a workspace.**

**(U) 3.2.2.4 The system shall allow the user to have multiple workspaces.**

**(U) 3.2.2.5 The system shall include a map widget.**

**(U) 3.2.2.18 The system shall be capable of operating widgets within widget frameworks.**

(U) The OZONE Widget Framework (OWF) is an example of a framework which supports widgets (also known as gadgets).

**(U)3.2.2.20 The SWIF server shall support commonly accepted Web technologies.**

(U) These technologies include patterns and interface protocols such as Asynchronous JavaScript and XML (AJAX), RESTful Web Services.

**(U) 3.2.2.27 The system shall include a collaboration widget.**

**(U) 3.2.2.28 The system shall include a link analysis widget.**

**(U) 3.2.2.29 The system shall include a graph visualization widget.**

(U) This widget supports charting operations to aid in visualizing data.

**(U) 3.2.2.30 The system shall include a data import widget.**

**(U) 3.2.2.31 The system shall provide a timeline widget.**

**(U) 3.2.2.32 The system shall provide an operations clock tool.**

**(U) 3.2.2.33 The system shall provide a decision matrix widget.**

**Section 3.2.3 (U) Roles and User Account Management**

**(U) 3.2.3.1 The system shall provide a Web-based user interface (UI) to support user account management (UAM) functionality.**

**(U) 3.2.3.2 The system shall provide the capability to use user account privileges to manage user access.**

**(U) 3.2.3.3 The system shall employ user roles that restrict user access to system functionality based on assigned roles.**

**(U) 3.2.3.4 The system shall provide a set of roles to allow users to have system access.**

(U) As a minimum, the system will have the following roles:

* Site Administrator
* Operator
* SSO
* ISSM/ISSO
* Viewer (read-only access)
* External System
* System
* Group Manager

**(U) 3.2.3.5 The system shall allow adding additional roles without requiring a major redesign of the system.**

**(U) 3.2.3.6 The system shall provide the capability to change a user’s assigned roles.**

**(U) 3.2.3.7 The system shall provide the capability to reset the passwords for existing user accounts.**

**(U) 3.2.3.8 The system shall notify the user via that user’s account-associated email address when the user’s password has changed.**

**(U) 3.2.3.9 The system shall provide a user account workflow to manage account creation.**

(U) Workflow steps will include security approval, account approval, and activation.

**(U) 3.2.3.10 The system shall support multiple states.**

(U) Acceptable values for account states and statuses include the following (read as State/Status):

* Active/Unlocked
* Active/Locked
* Inactive/Locked
* Inactive/Archived

**(U) 3.2.3.11 User accounts in the system shall be capable of being in only one state at any one time.**

(U) Account state includes the status of the account.

**(U) 3.2.3.12 The system shall retain all user accounts regardless of their current state.**

(U) The system will not delete user accounts from the system for historical purposes based on State/Status.

**(U) 3.2.3.13 The system shall provide the capability for viewing user accounts based on the account state.**

**(U) 3.2.3.14 The system shall assign a unique identifier to each user account.**

**(U) 3.2.3.15 The system shall require the use of strong passwords.**

(U) For this system a strong password must contain at least 15 characters, of which there are at least two uppercase letters, two lowercase letters, two numbers, and two symbols. In addition, a strong password cannot be the same as the user’s previous passwords, cannot include the user’s name, and is not your login.

**(U) 3.2.3.17 The system shall reject a password if the user tries to save a password that does not meet the strong password requirement.**

**(U) 3.2.3.18 The system shall lock a user account if the user fails three successive login attempts within a given timeframe.**

**(U) 3.2.3.19 The system shall allow only Administrators to unlock user accounts.**

**(U) 3.2.3.26 The system shall require all login IDs to be unique.**

**(U) 3.2.3.41 The system shall support the concept of an “alias” to hide the true name of the user.**

**(U) 3.2.3.42 The system shall provide the capability to disable system roles.**

(U) This includes for example, if a role is no longer needed

**Section 3.2.4 (U) Groups**

**(U) 3.2.4.1 The system shall provide the capability for users to manage groups of users.**

(U) This management capability includes creating groups.

**(U) 3.2.4.4 The system shall allow groups to be composed of individuals from multiple organizations.**

(U) This permits individuals from one or more organizations to comprise a group.

**Section 3.2.5 (U) Search**

**(U) 3.2.5.5 The system shall filter search results.**

(U) Criteria for filtering search results includes the submitting user’s access and clearance level.

**(U) 3.2.5.6 The system shall provide a keyword search capability.**

**Section 3.2.6 (U) Workflows and Queues**

**(U) 3.2.6.1 The system shall provide for a workflow capability.**

**(U) 3.2.6.12 The system shall provide the capability for a user to save a workflow.**

**(U) 3.2.6.15 The system shall be capable of storing multiple workflows.**

**Section 3.2.13 (U) Audit**

**(U) 3.2.13.1 The system shall record significant events in audit records.**

* Successful logon and logoff attempts by users.
* Unsuccessful logon and logoff attempts by users
* New user account creation

**Section 3.2.15 (U) System Configuration**

**(U) 3.2.15.1 The system shall provide a Web-based user interface (UI) to support System Configuration functionality.**

**(U) 3.2.15.2 The system shall restrict access to application configuration settings to privileged users designated as application administrators.**

(U) This normally is the *Administrator* role.

**(U) 3.2.15.3 The system shall provide the capability for an administrator to set configurations.**

(U) These settings, as a minimum, include the following:

* Configure User Account Management
* Set the system’s time zone; the default time zone normally should be Zulu
* Set the name of the site (installation)
* Reset passwords
* Set the system’s maximum classification
* Enter the location of external authentication servers to be used to verify clearance levels

**Section 3.2.16 (U) User Preferences**

**(U) 3.2.16.1 The system shall allow a user to configure the user’s preferences for data display.**

**(U) 3.2.16.9 The system shall allow a user to save the user’s preferences for workspace settings.**

**Section 3.2.17 (U) User Interface**

**(U) 3.2.17.1 The system shall provide a browser-based user interface (UI) to execute system functions.**

**(U) 3.2.17.2 The system user interface (UI) presented to the user shall be based on the user’s role.**

**(U) 3.2.17.6 The system shall use a CLOSE button (if in view mode) to close the current window.**

**(U) 3.2.17.13 The system user interface (UI) shall provide the capability for the user to associate entities using a drag-and-drop metaphor.**

**(U) 3.2.17.25 The system shall provide a feedback mechanism to the user to indicate the system is processing the user-requested action if the transaction requires more than two (2) seconds to respond.**

**Section 3.2.18 (U) Database**

**(U) 3.2.18.24 The system database shall store widget settings for each user preference (i.e. URL, size, shape, workspace, customization, dashboard configuration) .**

**Section 3.2.20 (U) Help**

**(U) 3.2.20.1 The system shall provide an online help capability.**

**Section 3.3 (U) SWIF Application Requirements**

**Section 3.3.1 (UFOUO) Planning Application**

**(U//FOUO) 3.3.1.1 The system shall include a Planning application.**

**(U//FOUO) 3.3.1.2 The system Planning application shall operate within the SWIF architecture.**

**(U//FOUO) 3.3.1.3 The system Planning application shall use the SWIF Common Services.**

(U) This includes interacting with the common services.

**(U//FOUO) 3.3.1.4 The system Planning application shall be capable of using the widgets within the SWIF Core Services.**

**(U//FOUO) 3.3.1.7 The system Planning application shall be capable of using the System and Common Services within the SWIF Common Services.**

**(U//FOUO) 3.3.1.30 The system shall provide the capability for a user to set discretionary access (users or groups) to the Planning Services.**

**(U//FOUO) 3.3.1.31 The system shall provide the capability for a user to develop a Concept of Operations (CONOP) for the selected capability specific to a Plan.**

**(U//FOUO) 3.3.1.34 The system shall provide the capability for a user to create a product from a Plan.**

(U) This includes creating a product from a Concept of Operations (CONOPS).

**Section 3.3.2 (U) Target Folder Application**

**(U) 3.3.2.1 The system shall include a Target Folder application.**

**(U) 3.3.2.2 The Target Folder application shall work with the SWIF core services.**

**Section 3.4.2 (U) Internal Interfaces**

**(U) 3.4.2.1 The system’s hardware interfaces shall be compliant with referenced operations and computer/communications security requirements and standards.**

**(U) 3.4.2.2 The system shall be capable of operating on Ethernet-based networks that support protocols including TCP/IP and HTTPS.**

**(U) 3.4.2.3.The system shall provide the capability to interface with a database.**

**(U) 3.4.2.4 The system shall provide for secure connections (TLS) for all thick client communication.**

**Section 3.4.3 (U) External Interfaces**

**(U) 3.4.3.4 The system shall provide for secure network connections (HTTPS) for all Web interfaces.**

(U) This requirement includes Web service methods.

**Section 3.8 (U) Security and Privacy Requirements**

**Section 3.8.1 (U) Security**

**(U) 3.8.1.4 The system shall be accessible only to authorized users.**

**(U) 3.8.1.5 The system shall require a user to log on to the system before the user can access the system application and its resources for any functionality.**

**(U) 3.8.1.7 The system shall allow for only a single session per user account.**

**(U) 3.8.1.10 The system shall include read-only classification banners within each user interface (UI) screen displayed.**

**(U) 3.8.1.12 The system shall allow the SWIF Administrator to configure the classification banner settings.**

**(U) 3.8.1.18 The system shall provide a role-based access control system to support a single log-on capability based on an individual user profile.**

(U) This process consists of strong identification and authorization and formal accesses (clearances).

**(U) 3.8.1.19 The system shall authenticate each user using strong authentication mechanisms over secure channels before authorizing access to the system.**

**(U) 3.8.1.23 The system shall restrict access to actions based on roles with associated privileges.**

**(U) 3.8.1.28 Each user shall log in and be authenticated on a trusted network on which SWIF resides**

**(U) 3.8.1.43 The system shall assign restrictive default values for the access control attributes of all subjects and objects when they are created.**

(U) For components supporting a MAC policy, the system shall assign the MAC attributes to the access control attributes for all subjects and objects as they are created. For components supporting a DAC policy, the system shall assign the DAC attributes to the access control attributes for all subjects and objects as they are created.

**(U) 3.8.1.44 The system shall assign the MAC attributes to the access control attributes for all subjects and objects residing on systems enforcing a MAC policy.**

**(U) 3.8.1.45 The system shall provide the capability for a subject to obtain the DAC attributes (e.g., group membership or access type) for a particular subject (user) or object they dominate.**

**(U) 3.8.1.46 The system shall provide the ability for a subject residing on systems enforcing a MAC policy to obtain the MAC attribute values of a subject or object they dominate.**

**(U) 3.8.1.47 The system shall provide the ability for a subject to determine whether it has DAC access to a named object.**

**(U) 3.8.1.48 The system shall be able to compare two sets of MAC attribute values to determine their dominance relationship.**

**(U) 3.8.1.49 The system shall be able to determine whether the values for the MAC attributes assigned to a subject or object are valid, to include conforming to the relationship rules for MAC attributes.**

**(U) 3.8.1.60 The system shall store generated audit events into an audit log that is protected against unauthorized modification.**

**(U) 3.8.1.61 The audit log shall be capable of being exported by authorized privileged users.**

(U) This includes the ability of an authorized privileged user to print the audit log.

**(U) 3.8.1.67 The systems shall be capable of being restored to the last known secure configuration through the application of the recorded changes to security-relevant data including functions.**

**(U) 3.8.1.76 The system shall invoke the appropriate user interface based on user authentication.**

(U) This occurs after General and Privileged Users have successfully identified and authenticated themselves and have selected a role.

**Section 3.10 (U) Computer Resource Requirements**

**Section 3.10.3 (U) Computer Software Requirements**

**(U) 3.10.3.1 The system shall operate, as a minimum, on two servers.**

(U) The current minimum system application and the database servers are the following.

* Tomcat Web Application or Servlet Server
* Mongo Database Server

**(U) 3.10.3.2 The system server shall support cross-platform deployment.**

(U) Cross-platform deployment includes, for example, deployment on a WinOS or Linux-based operating system in addition to OS-X.

* OS X Requirements:
* OS X Version 10.6 (Snow Leopard)
* Windows Operating System Requirements:
* Windows 7
* Windows Server 2003/2008/2012
* Linux Requirements
* Red Hat Enterprise Linux (RHEL)
* Community Enterprise Operating System (CENTOS)
* Secure Linux (SELinux)
* Fedora

**(U) 3.10.3.3 The system shall support multiple browsers.**

(U) The system currently supports the following browsers:

* Safari
* Chrome
* Firefox

**(U) 3.10.3.4 The system shall deny access by users who attempt to access the system using a Web browser that has not been approved by the target network Chief Information Officer (CIO).**

**Section 3.11.4 (U) Maintainability**

**(U) 3.11.4.5 The system shall be implemented in a layered architecture.**

**Section 3.11.6 (U) Portability**

**(U)3.11.6.1 The system software shall be capable of being migrated to more powerful processing platforms in support of an expanded user capacity.**

**(U)** **3.11.6.2 The system shall be capable of running on a Linux operating system.**

**(U)** **3.11.6.3 The system shall be capable of running on a Mac operating system.**

**(U)** **3.11.6.4 The system shall be capable of running on a Fedora operating system.**

**Section 3.11.7 (U) Reusability**

**(U)** **3.11.7.1 Reusability shall be considered in the design of SWIF.**

**(U) 3.11.7.2 The architecture of service components for SWIF shall consider existing APIs.**

(U) Consider Open Standards in addition to existing APIs.

**Section 3.11.9 (U) Usability**

**3.11.9.5 The system help functionality shall be easy to locate.**

**Section 3.11.12 (U) Design and Construction Constraints**

**(U)** **3.12.5 The system shall be capable of operating within the OZONE Widget Framework OWF environment.**

# (U) NOTES

## (U) Acronyms and Abbreviations

|  |  |
| --- | --- |
| **Acronym** | **Expansion** |
| ABAC | Attribute Based Access Control |
| ADAAG | Americans with Disabilities Act Accessibility Guidelines |
| AJAX | Asynchronous JavaScript and XML |
| APG | Automated Password Generator |
| CAPCO | Controlled Access Program Coordination Office |
| CAS | Central Authentication Service |
| CDM | Common Data Model |
| CENTOS | Community Enterprise Operating System |
| CLI | Call Level Interface |
| CM | Configuration Management |
| CMP | Configuration Management Plan |
| COMSEC | Communications Security |
| CONOPS | Concept of Operations |
| COTS | Commercial-Off-The-Shelf |
| CRUDA | Create, Read, Update, Delete, Archive |
| CSCI | Computer Software Configuration Item |
| CV | Conceptual View |
| DAA | Designated Approving Authority |
| DAC | Discretionary Access Control |
| DBDD | Database Design Description |
| DCADS | Defense Contract Action Data System |
| DCO | Defense Connect Online |
| DIACAP | DoD Information Assurance Certification and Accreditation Process |
| DID | Data Item Description |
| DMS | Degrees Minutes Seconds |
| DoD | Department of Defense |
| DODAF | DoD Architecture Framework |
| DODD | DoD Directive |
| DT&E | Developmental Test and Evaluation |
| ELB | Elastic Load Balancing |
| EPO | Engineering Process Office |
| FIPS | Federal Information Processing Standards |
|  |  |
|  |  |
| FISMA | Federal Information Security Management Act |
| GIS | Geographic Information System |
| GML | Geography Markup Language |
| GOSS | Government Open Source Software |
| GOTS | Government-Off-The-Shelf |
| HA | High Availability |
| HTTPS | Hypertext Transfer Protocol Secure |
| HWCI | Hardware Configuration Item |
| IA | Information Assurance |
| ICD | Intelligence Community Directive |
| ICD | Interface Control Document |
| IC ISM | Intelligence Community Metadata Standard for Information Security Marking |
| ICITE | Intelligence Community Information Technology Enterprise |
| IDD | Interface Design Description |
| INFOSEC | Information Security |
| IP | Internet Protocol |
| IPT | Integrated Product Team |
| IRS | Interface Requirements Specification |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| JDBC | Java Database Connectivity |
| JNDI | Java Naming and Directory Interface |
| JTA | Java Transaction API |
| JITC | Joint Interoperability Test Command |
| LDAP | Lightweight Directory Access Protocol |
| LDM | Logical Data Model |
| MAC | Mandatory Access Control |
| MIDB | Modernized Integrated Data Base |
| MCMT | Mean Corrective Maintenance Time |
| MGRS | Military Grid Reference System |
| MIL-HDBK | Military Handbook |
| MILSTD | Military Standard |
| MMCT | Mean Maximum Corrective Time |
| MTBF | Mean Time Between Failures |
| MTTR | Mean Time to Repair |
| NAI | Named Area of Interest |
| NSS | National Security Systems |
| NTDS | Naval Tactical Data System |
| NTK | Need to Know |
| OS | Operating System |
| OSHA | Occupational Safety and Health Administration |
| OT&E | Operational Test and Evaluation |
| OV | Operational View |
| OWF | OZONE Widget Framework |
| PKI | Public Key Infrastructure |
| PL | Public Law |
| PL | Protection Level |
| PM | Program Manager |
| RHEL | Red Hat Enterprise Linux |
| RUP | Rational Unified Process |
| QOS | Quality of Service |
| SDD | Software Design Description |
| SDP | Software Development Plan |
| SLA | Service Level Agreement |
| SMTP | Simple Mail Transfer Protocol |
| SPAA | Standard Process Assets Architecture |
| SPAWAR | Space and Naval Warfare |
| SQL | Structured Query Language |
| SRR | Security Readiness Review |
| SRS | Software Requirements Specification |
| SSC | SPAWAR Systems Center |
| SSDD | System/Subsystem Design Description |
| SSAA | System Security Authorization Agreement |
| SSS | System/Subsystem Specification |
| STIG | Security Technical Implementation Guide |
| SWIF | Secure Web Integration Framework |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| TSCM | Technical Surveillance countermeasures |
| UAM | User Account Management |
| UFAS | Uniform Federal Accessibility Standards |
| UI | User Interface |
| UPA | Usage and Performance Analytics |
| UTM | Universal Transverse Mercator |
| VM | Virtual Machine |
| VOIP | Voice Over Internet Protocol |
| WFS | Web Feature Service |
| WMS | Web Map Service |
| WPS | Web Processing Service |
| XML | eXtensible Markup Language |

## (U) Definitions Used in this Document

*[Table is Unclassified]*

| **Term** | **Definition** |
| --- | --- |
| Capabilities | A term used to represent various combinations of tools, data, and processes. |
| CONOPS | A verbal or graphic statement that clearly and concisely expresses what the joint force commander intends to accomplish and how it will be done using  available resources. |
| Domain | A sphere of activity, concern, or function. |
| Entity | Something that exists as a particular and discrete unit within the system, e.g. object, group/unit, individual, geospatial area. |
| External System | A system role assigned to user accounts that are external systems enabling those systems to access specific SWIF web services. |
| General User | A system role whereby the user can access all system functionality that is not administrative in nature and that is authorized for their organization. This will be constrictive in nature and is based on their type of organization. All roles within SWIF are General User roles with exception of Site Administrators. |
| Group Manager | A system role whereby the user can perform CRUDA operations for Groups. Group Managers are privileged users with the authorization to set discretionary access to work products, workflows and queues within the system. |
| Groups | Two or more system users assembled around a topic of common interest. For SWIF, groups can be used to restrict access to domain-specific programs, system functionality, work products, etc. |
| ISSM/ISSO | A system role whereby the user functions as the activity’s focal point and principal advisor for INFOSEC matters on behalf of the Designated Approving Authority (DAA). The ISSM reports to the DAA and implements the overall INFOSEC program approved by the DAA. An activity may have multiple ISSMs. An ISSO is a system role whereby the user acts on behalf of the ISSM to ensure compliance with the INFOSEC procedures at the operational site or facility. The ISSM is responsible for performing those duties normally performed by ISSOs in the event that no ISSOs are appointed at the particular Command. This role is a privileged user role allowing access to security-relevant functions and data, including audit logs. |
| Operator | A system role whereby the user can perform the full scope of create, read, update, delete, archive (CRUDA) operations within the system with exception of administrative tasks. |
| Privileged User | A system role whereby the user can access all system functionality, including administration, authorized for the system. Privileged user roles include Site Administrator, ISSM/ISSO, SSO, and Group Manager. |
| Program | A set of activities with specific goal that is protected with security protocols providing [highly classified information](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States) with safeguards and access restrictions that exceed those for regular (collateral) classified information. |
| Site Administrator | A system role whereby the user is responsible for site-level administrative tasks that encompass the host site and that impact all using organizations. |
| SSO | A system role whereby the user verifies the security clearance of the individual requesting access to the SWIF system. The SSO will verify the requester’s clearance level, compartments, and releasability information. This role is a privileged user role allowing access to security-relevant functions and data, including audit logs. A user with this role is also authorized to |
| System User | This system role is reserved for internal system component actions only and is not available for assignment to users. |
| Tester | A system role whereby the user can perform test activities and access test tools within the system. |
| Viewer | A system role whereby the user can perform read-only operations within the system with exception of administrative tasks. |
| Work Product | Deliverable that must be produced to complete a project and achieve its objectives. Within the SWIF architecture, Work Products are those deliverable documents generated by users and groups using the domain-specific applications. |
| Target Folder | A folder, hardcopy or electronic, containing target intelligence and related materials prepared for planning and executing action against a specific target. |

## (U) REQUIREMENTS VERIFICATION Process

(U) The following information supplements the Qualification Provisions in Section 4.

(U) The SWIF Requirements Verification process will involve actual performance testing for each version release. The SWIF developer will verify conformance with the functional and performance requirements of Section 3 of this requirements document. The verification methods defined in Section 4 will be applied at appropriate locations and levels of assembly up to and including a fully configured SWIF architecture. Verification levels, including Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E) are not yet defined.

## (u) Requirements Implementation Order Option

(U) This section is included in the SSS as a Software Development Plan (SDP) does not yet exist for the SWIF Program. The following image shows one option for the order that components/requirements could be implemented. A “Phase” could consist of one long spiral or several short development cycles depending on the priority of the SWIF program management. The versions listed are only notional. Many components can be developed over a series of cycles/versions as well. This image is not intended to represent a schedule or act as the definitive order in which to implement requirements. *This diagram is only intended to act as an example of only one option in implementing requirements.*



*[Figure is* ***U//FOUO****]*

Figure : (U) Notional Example Representation of Requirement Implementation Order