Columbia River CROSSING

Road Map Item #: 5.2

Product Name: **DOCUMENT CONTROL PLAN**

PMP Appendix: APPENDIX L

Submittal Date: May 1, 2013

ABSTRACT: This deliverable describes the manner in which records of the CRC Program will be managed, controlled, and maintained in accordance with technical, management, and legal requirements.

DOCUMENT CONTROL PLAN

Draft Report

May 2013

Columbia River CROSSING

Title VI

The Columbia River Crossing project team ensures full compliance with Title VI of the Civil Rights Act of 1964 by prohibiting discrimination against any person on the basis of race, color, national origin or sex in the provision of benefits and services resulting from its federally assisted programs and activities. For questions regarding WSDOT's Title VI Program, you may contact the Department's Title VI Coordinator at (360) 705-7098. For questions regarding ODOT's Title VI Program, you may contact the Department's Civil Rights Office at (503) 986-4350.

Americans with Disabilities Act (ADA) Information

If you would like copies of this document in an alternative format, please call the Columbia River Crossing (CRC) project office at (360) 737-2726 or (503) 256-2726. Persons who are deaf or hard of hearing may contact the CRC project through the Telecommunications Relay Service by dialing 7-1-1.

¿Habla usted español? La informacion en esta publicación se puede traducir para usted. Para solicitar los servicios de traducción favor de llamar al (503) 731-4128.

TABLE OF CONTENTS

Attachments

1. Introduction

1.1 Purpose

The purpose of this Document Control Plan is to describe the manner in which records of the CRC Program will be managed, controlled, and maintained in accordance with technical, management, and legal requirements. Document control and records management procedures are used to handle, maintain, and manage all documents and supporting information, as well as contractual documents, financial records, and grant-related records throughout the design and construction phases of the Program. Document control and records management tasks include: receipt, storage, retrieval, and distribution of all project documents, including key project documents classified as "controlled documents."

The CRC's document control and records management system includes the Prolog database to monitor dates of receipt, transmittal, and final disposition of project management, financial, procurement, right-of-way, quality, environmental compliance, and reference documents and legal records. It also includes ProjectWise software for the purpose of managing, retrieving, and sharing original engineering CAD drawings, as-built drawings, and various design records.

1.2 Scope

For purposes of this plan a "document" is any electronic or hardcopy media designed to convey information about or on behalf of a project, including but not limited to meeting documentation, deliverables, drawings, electronic mail, faxes, letters, memoranda, organizational charts, pictures, presentations, project binders, reports, specifications, and spreadsheets.

Document management achieves the following objectives:

- Provide safe storage of all documents in the project files.
- Provide clarity regarding which version of a document and/or deliverable is the latest version.
- Provide easy and controlled access to project documents to project staff.
- Provide a record of approved deliverables over the life of the project.
- Provide security measures to maintain restricted access to confidential documents.
- Provide an accurate and complete archive of project documents to the organization at the end of the project.

1.3 References

- CRC Project Management Plan

- CRC ProjectWise Management Plan
- CRC Public Disclosure Procedure
- RCW 42.56 Washington Public Records Act
- ORS 192. Oregon Records, Public Reports and Meetings

1.4 Document Maintenance

This document will be reviewed regularly and updated, as needed, as the project proceeds through each phase of its life cycle.

This document contains a revision history log. When changes occur, are reviewed and approved, the document's revision history log will include an updated version number, the revision date, the owner making the change, and a high-level description of the change(s) made.

2. Organization and Responsibilities

2.1 Project Director

The CRC Project Director(s) are responsible for implementing and enforcing the provisions of the CRC Project Management Plan (PMP), project procedures, project subplans and for appointing staff persons to serve as managers and coordinators.

2.2 Document Control Manager

The Document Control Manager reports to the Project Controls Manager and is responsible for document control and record management of the official project files, with the exception of engineering design drawings. The Document Control Manager oversees the day-to-day document control and record management duties including the facilitation of capturing, properly indexing, securing, archiving, versioning, and keeping the project documents current.

2.3 Public Disclosure Lead

The Public Disclosure Lead reports to the WSDOT Records & Information Services Manager and is responsible for responding to public records requests. The document Controls Manager provides support in finding and providing documents to the CRC Public Disclosure Coordinator and Public Disclosure Lead for responses to public records requests.

2.4 CAD Manager

The CAD Manager is responsible for the day-to-day management of CRC engineering design drawings.

2.5 CRC Project Team Members

All project staff members, including state employees and onsite consultants, are responsible for conveying newly created and required documents to the Document Control Staff to be retained in the project files.

2.6 Non Disclosure Agreement (NDA) Team

For each situation where confidential documents, subject to non-disclosure requirements, are identified, a list of participants (the non disclosure agreement team (NDA) that will be required to sign a non disclosure agreement) will be developed. Each NDA Team is specific to a non-disclosure agreement and will have different titles, team lead and members, depending on the purpose of the team's agreement.

2.7 Field Office Project Team

Field office records and related documents will be maintained by the Resident Engineer within the appropriate office. The Resident Engineer will coordinate conveyance of any documents required by the CRC Program office to Document Control for program level retention.

2.8 WSDOT IT

WSDOT IT department is responsible for maintaining the functionality and data integrity of all database applications.

3. Management of Project Records

Records management generally refers to the management of records as they are created or received and used and maintained, and which may or may not be subject to formal document control, as well as the proper disposition of inactive documents when they are no longer needed and the retention periods have lapsed. In general, materials published by another organization in a public location (e.g., Internet) are not retained as project documentation. In addition, some project related documentation may be retained by a partner entity that is responsible for all legal ramifications of the documents as in the case of right of way documentation and contractual documents. In these instances a determination will be made as to what content should also reside in the CRC project management office.

3.1 Document Control System

The purpose of Document Control is to maintain accurate records that reflect the CRC business functions, policies, decisions, transactions and operations, and to capture and retain records that are subject to the retention requirements of Public Records Laws of the two States. Along these lines, the Document Control system helps to facilitate the capture, indexing, securing, archiving, and versioning of project documents.

Meridian's Prolog Manager Application is the primary system that is used to electronically track all non Architectural and Engineering CRC records. Prolog Manager was designed for the construction industry and is being utilized to meet the demands of CRC Program as well as its construction projects.

The Document Control System is composed of designated document control staff, document control (Doc Ctrl) records and related procedures. Document Control Staff enter records into the Document Control System and link where appropriate the electronic file to the record.

Some records may exist outside of the Document Control System and are maintained in various departmental paper or electronic filing systems of the two STATES. Retention and disposition of these records are still subject to state and federal records retention requirements.

3.2 Project Records

This section describes document control processes and responsibilities that will be followed and/or executed by the CRC Program.

Active records include those documents, records, and supporting information that are produced or received during the development, planning, design, construction, and closeout of the CRC Project. A variety of documents are subject to formal controlled distribution, as specified in the Controlled Documents section of the CRC Document Control procedure. In addition, supporting information such as calculations and analysis, and other documentation must also be maintained. In some cases, records are maintained separately for legal and regulatory reasons.

To ensure adherence with the overall document control goals, staff have identified three primary types of documents:

- Reference material.
- Project work papers.
- Official project files.

Reference Material

Reference material includes any document (electronic or physical) that is not a direct product of the CRC Team or not produced for the CRC Program, but is helpful or necessary in order to perform project functions. Reference material will be included in its own section of the program filing structure and will not follow the traditional WBS structure as designated for official program files.

The initiator of the reference material should coordinate with Document Control to determine the most appropriate placement of the information within the project library, thereby making the material available for all team members.

Project Work Papers

Project work papers include any document or file that is a direct product of the CRC project, but that is not in its final or distribution draft format. Project work papers generally require further collaboration or processing among team members. Ultimately naming conventions and disposition of work products are the responsibility of the task area lead.

Official Project Files

An official project file is generally a product of the CRC Program. It can be either electronic or paper, and is in its final form. Final form includes drafts that are issued for review. Common, well-known examples of official project files include:

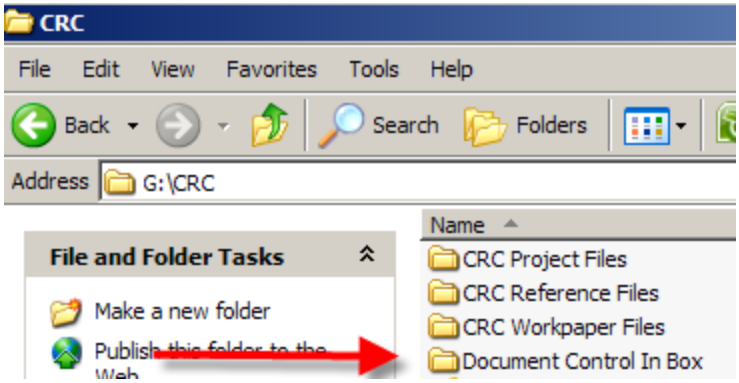
- **Project Management Records** – Schedules, transmittal documents, Project Management Plan (PMP), Procedures Manual, reports, correspondence, analysis, and other records related to the management of the CRC Program.
- **Financial Records** – Financial and grant-related records and those associated with agreements, contracts, payments and financial reporting.
- **Procurement Records** – Pre-solicitation documents, solicitations/addenda/ amendments, statements of work/scopes of service, notices of award, records of any protest, bid/performance/payment or other bond documents and notices to sureties, notices to proceed, contract amendments and subcontract modifications, and construction administration records.
- **Right-of-Way Records** – The right-of-way manager is responsible for conveying the appropriate level of project ROW documentation to the Document Control team.
- **Design Records** – Engineering and design reports, including supporting analysis and records, whether prepared on-site or by off-site consultants and contractors.

- **Construction Records** – Construction-related records and documents will be maintained by the responsible Resident Engineer within the appropriate project package.
- **Quality Records** – Objective evidence of quality, in accordance with FHWA and FTA QA/QC guidelines, during design and construction.
- **Environmental Compliance Records** – Analysis, correspondence, reports, and other documents associated with environmental site assessments, environmental analysis, environmental impact statements, environmental mitigation including monitoring reports, and submittals to federal, state, and local regulatory agencies. The Environmental manager is responsible for ensuring that the official environmental permits, the Biological Opinion, and compliance records and reports are turned over to the Document Control team for inclusion in the official project record.
- **Other Records** – Other important records and documents produced by outside or internal sources including e-mail communications, photos, and presentations. Generally, these documents are distributed as appropriate.

3.3 Project File Processes

If a document is produced internally it should be printed to PDF by the responsible staff and submitted to document control in one of the following methods:

1. Place the electronic document in the Document Control Electronic Inbox on the G:Drive and send an email to document control providing relevant information for the document to facilitate correct filing:



Or

2. Email the document to Document.Control@ColumbiaRiverCrossing.org . This method should not be used with large file size documents. If the documents are large or it is impractical to place them in the Document Control Inbox as described in 1. above, please email a link to Document Control.

If the document has been produced outside the office, every attempt should be made to obtain an electronic copy of the document. If this is not feasible, then the hardcopy document should be provided to Document Control for scanning and uploading into the Document Control System.

Once the document is retrieved and or scanned, the file will be renamed using the appropriate file storage structure and logged into the Prolog tracking system.

3.3.1 Hardcopy Correspondence

Incoming

1. All incoming hardcopy documents are received by the front desk personnel.
2. The front desk personnel sorts and stamps incoming hardcopy documents with the date received.
3. The front desk personnel scans the document except when scanning is not feasible.
4. The front desk personnel logs receipt of the hardcopy document in the Excel based form.
5. After logging, the front desk personnel should email the electronic copy of the mail to the individual to whom the document was addressed and copy Document Control.
6. Document control will log the document as received and capture the distribution list indicating who received the document from front desk personnel.
7. If the incoming document/correspondence item includes action items, it is the responsibility of the recipient to notify Document Control so that action can be assigned within the document record.

Outgoing

1. Project team members who send hardcopy correspondence are responsible for scanning the item and providing electronic copies or sending copies of the documents/correspondence to Document Control.
2. Document control will log the correspondence within Prolog and will capture information regarding the sender along with intended recipients.

3.3.2 Electronic Correspondence

Incoming

1. Project team members who receive incoming electronic mail are responsible for determining whether the document should be included in the official Project Files.
2. If so, the recipient should forward the mail Document Control.
3. Upon receipt, Document Control will log the item in Prolog along with the recipients and senders.

4. Any attachments to the email are automatically uploaded into the Project File within Prolog.

5. If the incoming item includes action items, it is the responsibility of the recipient to follow through on the action.

Outgoing

Project team members who send electronic correspondence are responsible for making a determination of whether the email should be included in the official project file.

1. If the outgoing mail is pertinent to the project file then the sender should copy Document Control on the email or forward the email to Document Control.

2. Upon receipt, Document Control will log the item in Prolog along with the recipients and senders.

3. Any attachments to the email are automatically uploaded into the Project Files within Prolog.

3.3.3 Email used to Transmit Documents

1. The document that will be transmitted should already reside within the official project files. All documents should be transmitted from within Prolog. If the individual does not have access to Prolog they should coordinate with the Document Control Team to send on their behalf.

2. Prolog will automatically create a transmittal record associated with transmitted documents for all documents sent from within Prolog.

3.4 Architectural and Engineering (A & E) Drawings

Architectural and Engineering drawings are the responsibility of the CAD manager. Management of these drawings is provided in the CRC ProjectWise Management Plan.

3.5 Web Publicized Documents Including Wiki Site Documents

It is important to maintain copies of all information posted on the website, including the dates it was available to the public.

3.5.1 Web Publicized Documents Process

1) For each update to the project website there should be a transmittal created within Prolog to show the information that is being placed on the web. The recipient identified on the transmittal will be “CRCWebsite.”

2) If the information is text the following information about the text should be transmitted to the Webpage:

   a) The actual text.

b) Any necessary context that explains the text.

c) Who if anyone, approved or requested the information to be placed on the web.

d) The date that the information was placed on the web.

e) Any information that is being superseded, changed or removed as a result of the new text.

3) If the item is a document or graphic the following should be transmitted to the recipient "CRCWebsite" and linked to the document within the Project Files.

a) No document should reside on the web that does not reside in the Project Files.

4) Within the transmittal the following information should be included:

a) Any necessary context that explains the document and the need for its placement.

b) Who if anyone approved or requested the document to be placed on the web.

c) The date that the document was placed on the web.

5) If a document or graphic is being removed from the webpage a note should be made on the original transmittal that states the date that it was removed.

3.6 Non Disclosure Agreements (NDA)

The intent of the Non Disclosure Agreement (NDA) document designation is to prevent any unauthorized exchange, distribution, or disclosure of documents covered under an NDA agreement. The CRC project has identified two types of NDA documents that need to be protected:

1. Internal NDA agreements – These are agreements that cover internal project work products such as Request for Qualifications and Request for Proposals.
2. Third Party NDA agreements – These are agreements that are entered into by the project and parties outside the project whereby the outside party wishes to protect the documents that they share with the project.

Different procedures based on the type of NDA are covered in the sections below.

3.6.1 Internal NDA Agreements

Internal NDA agreements are signed by project team members as a reminder that they are not to exchange, distribute or disclose any of the documents covered by the NDA. Once the agreement has been signed the NDA agreement will be sent to Document Control to be placed in the official project file.

3.6.2 Third Party NDA Agreements

The designated NDA Team lead is responsible for the care and disposition of these documents as outlined below.

Definition

Work products - include any document or file that is a direct product of the CRC NDA team and may require further collaboration or processing among team members.

Repository Files – include any document that was obtained from the protected parties and will be stored as a reference for NDA team work products.

ProjectWise Is a software application that will be utilized for the storage and collaboration between NDA team members for work products and repository files.

NDA Team –each NDA Team is specific to a non-disclosure agreement and will have different titles and members depending on the purpose of the team's agreement.

Restrictions on Access to Records

The intent of the Non-Disclosure Agreement is to prevent any unauthorized exchange, distribution, or disclosure of NDA documents by authorized NDA team members. **Only NDA team members and any required repository administrators will have access to NDA team documents.**

Examined Documents

Each NDA team will keep a NDA Document Log. Every document examined should be included in the log irrespective of whether or not the document was retained for the team files. It is important to enter enough information in the log so that the document can be located at a future date even if it is not initially retained.

Repository Files

A complete library of retained files shall be included in the electronic repository. The electronic repository for NDA teams will be ProjectWise. **Only individuals who have been designated as NDA team members by the NDA team lead will be given permissions or access to ProjectWise by the CRC ProjectWise administrator.**

Once the NDA team has determined that a copy of the examined files will be retained for the repository, the document will be scanned and uploaded into the NDA team user folders within the ProjectWise system. ProjectWise upload security rights are limited to the NDA team lead. Team members have view rights only. The Document should be named with its unique document ID as discussed below under NDA Document Log. The document ID should be consistent for each location in which the document is stored.

At no time will any repository electronic NDA document be downloaded and stored on a team member's local computer or other storage device. (Note: ProjectWise securities are set to automatically purge the file from the local computer once it is freed, closed or printed) Viewing of repository documents is to be limited to two purposes:

1. Viewing and reading the document
2. Printing the document for placement in an approved hardcopy filing location

Once a file has been placed in the repository, it cannot be deleted until dissolution of the NDA team.

NDA Document Log

There will be one central log of all documents examined and retained. The log will be stored in ProjectWise and should be updated continually to represent the most current disposition of all documents examined or stored and any hard copy location. Once an item is entered into the log it remains in the log until the end of the NDA team. At a minimum the log will contain the following:

Examination Phase

1. Date of the initial examination of the document
2. A unique identifier for the document that will be used for the duration of the NDA team
3. Document type (example correspondence, report, engineering drawings, contract etc.)
4. Identifying characteristics of the document – examples include a document date, To and From, Report title, drawing number or any other information that could assist in the future retrieval of the document if it were not retained for the repository
5. Document context
6. Team members who viewed the document

Repository

7. Person who authorized placement of the document in the NDA team electronic repository (note this should be the NDA team lead)
8. Each authorized hardcopy location of the document and the date it was placed

Work Products

All works in progress should be saved in the ProjectWise so that they are accessible by NDA team members. Collaboration will be accomplished utilizing a check out / check in process that provides a trail of edits and commenting for each work product until which time the product is submitted for outside NDA team review or for final.

A log of all NDA work products will be maintained in the ProjectWise NDA team work product user folders and will contain each of the following:

1. A unique ID that will be used in all locations to identify the exact document
2. The document version
3. The document date
4. Author name(s)
5. Type of Document

The NDA team lead will be responsible for documenting each team member and their security rights for adding, deleting and editing work in process. This documentation will be provided to the ProjectWise administrator so that he or she can set up database securities accordingly.

Hardcopy Locations

Hardcopies will be maintained in NDA team approved filing locations. In order to be NDA approved, the file cabinet must be locked. Each approved hardcopy file location will contain a copy of the NDA document log that is maintained within ProjectWise. Each time a hard copy is added to an approved location the individual must provide a date that the document was added to that location in the NDA document log. The log should then be printed and placed in the files as the most current representation of the file contents and their disposition:

Compliance Audits

The CRC project may conduct compliance audits to ensure the procedures outlined herein are being preserved.

Public Disclosure

The record contents which are the subject of confidentiality agreements, which otherwise would be subject to provision under Chapter 42.56 RCW (the Public Records Act) may be enjoined or exempt from provision as allowed by RCW 42.56.270, RCW 42.56.540, and RCW 19.108.010(4).

3.7 Sensitive Security Information (SSI)

SSI is any information or record whose disclosure may compromise the security of the traveling public, transit or state employees, or transit or highway infrastructure. SSI may include data, documents, engineering drawings and specifications, and other records whose disclosure could increase the agency's risk of harm. For example, threat and vulnerability assessments are SSI. Management and handling of SSI documents is outlined in the SSI Process below:

3.7.1 Identifying and Designating SSI

Any program employees who would reasonably be expected to create records that might contain SSI should be able to evaluate those records for potential SSI content.

If a record potentially contains SSI, the employee should refer it to the Document Controls Manager for making SSI determinations.

To determine whether information could be SSI, transit agency employees should consider the threat environment within their operating areas and around their facilities and infrastructure as well as the following:

- Does the public need to know this information? For example, for safety reasons, transit agencies must share emergency evacuation and response plans with a wide audience. Categorizing such information as SSI could discourage its distribution.

- Is the same or similar information readily available from other sources? For example, the location of a closed-circuit television (CCTV) camera that is in plain sight in a transit facility is not SSI, whereas a map showing the locations of all CCTV cameras in a transit system might be SSI.

- Could someone intent on causing harm misuse the information? For example, could someone use it to target facilities or operations? Does the information increase the attractiveness of a target or place transit agency infrastructure or operations at greater risk of threats?

General principles that individuals and committees can use for identifying whether records should be categorized as SSI include:

- Base identification of SSI on the regulatory definition and types of SSI listed in 49 CFR Parts 15 and 1520.

- Do not categorize as SSI information relating to the environment, safety, or health unless security requirements significantly outweigh the public's need to know.

- Do not categorize records as SSI out of convenience or a desire to keep them private.

- Do not use SSI to conceal or delay the discovery of regulatory violations, errors, or inefficiencies; to avoid embarrassment; or to restrain competition.

- Categorize records as SSI only if record-holders can be notified of the categorization, and the SSI can be uniformly protected. The individual or committee making the designation is responsible for notifying holders.

If only a portion of a document is SSI, the program must categorize and control the entire document as SSI. To release the document, the program must first redact the SSI from it.

3.7.2 Marking SSI

SSI records require a protective marking and a distribution limitation statement to inform users of their security-sensitive nature and the need to protect them from unauthorized distribution as defined in 49 CFR §15.13 and §1520.13.

SSI records in both printed and electronic form must be marked as follows:

SENSITIVE SECURITY INFORMATION

and must include the distribution limitation statement specified in the regulation:

> *Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation*

Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

For paper SSI records, the protective marking must appear at the top of every page, including the outside front and back covers, binder covers, and title pages; and the distribution limitation statement must be at the bottom of every page, including the outside front and back covers, binder covers, and title pages. The protective marking should be printed or stamped in a font size larger than the text of the record. Electronic documents must be similarly marked and the distribution limitation statement included on every page. Attachment A-2 contains sample front and back-cover pages for paper or electronic SSI.

For non-paper SSI records such as videotape and audio recordings, the protective marking and the distribution limitation statement must appear clearly and conspicuously on the record so that the viewer or listener is reasonably likely to see or hear them. In addition, non-paper SSI records should be kept in containers that are clearly marked on the outside.

Floppy disks, CDs, DVDs, tapes, and other media on which electronic SSI is stored should also be marked, either directly on the medium or as a label attached to it. Alternatively, the media can be stored in marked containers.

SSI records may also be stored electronically on thumb drives. Federal Transit Administration (FTA) strongly recommends that SSI on thumb drives be password-protected or encrypted. However, the thumb drives should not have any SSI marking on them.

3.7.3 Accessing SSI

Access to SSI records must be controlled to prevent unintended disclosure. Restricting access to SSI means allowing only covered persons with a "need to know" to access them.

Only persons with a "need to know" may access SSI. Regulations at 49 CFR §15.11 and §1520.11 describe "need to know" in relation to a person who needs access to SSI in order to:

- Perform official duties, for example, pursuant to a contract or grant.
- Carry out, or supervise or manage persons who are carrying out, DHS- or DOT-approved, accepted, funded, recommended, or directed transportation security activities, or complete training to carry out such activities.
- Provide technical or legal advice to a "covered" person regarding transportation-security federal legal or regulatory requirements or in connection with a judicial or administrative proceeding regarding these requirements.
- Because having a need to know is the only way in which an employee, contractor, or vendor can gain access to SSI, transit agencies should define their "need to know" requirements as a matter of policy to assure that all persons can access the information they need to perform their jobs.

Additional information on covered persons can be found in the FTA Resource Document referenced in "C. References," above.

3.7.4 Controlling SSI

Storage – The following apply to the CRC program:

- If possible, the owner or originator of the SSI should store it.
- Each department or person may have a designated storage area for paper SSI.
- To preclude unauthorized access, SSI records should be stored in locked receptacles, such as file cabinets or desks unless the records are under direct supervision (that is, someone is working on them).
- SSI in electronic form on personal computers (PCs), floppy disks, CDs, DVD, tapes, or other electronic media should be password protected.
- The CRC information services personnel will establish electronic storage for SSI electronic documents accessible to those with a need for access.

Use – The following apply to the CRC program:

- During use, SSI records should not be left out in the open. For example, if a person using paper SSI records must temporarily leave the area of use, he or she may protect the SSI by storing the records in a locked drawer.
- Persons with knowledge of SSI should maintain vigilance when discussing SSI in meetings, on the telephone, or via radio.
- SSI should not be discussed in public conveyances or other locations that permit interception by unauthorized individuals.

Reproduction – The following apply to the CRC program:

- SSI records may be reproduced only to the extent necessary to carry out program business.
- Reproduced SSI must be marked and protected in the same manner as the original SSI. For example, persons photocopying paper SSI should make only the minimum number of copies needed.
- Copy machine malfunctions should be cleared and all paper paths checked for SSI. Excess paper containing SSI should be shredded.

Transmission – The following apply to the CRC program:

- SSI can be sent to “known” persons, addresses, or locations on the basis of the receiver’s “need to know.” However, persons sending SSI must assure against unauthorized disclosure.
- Within the program, transit agency, paper or electronic SSI, such as floppy disks and CDs, may be sent through interoffice mail with use of a standard internal distribution

envelope. In addition, the sender may hand-carry the SSI to another person or location.

- Sending paper or electronic SSI records outside of the program requires packaging in a single, opaque envelope or wrapping. The sender may use any mail method or courier service to transmit the information, as well as any commercial carrier. In addition, the sender may hand carry the SSI (for example, in a purse or briefcase) as long as he/she can control access to it.

- Transmission of SSI by telecommunications, such as telephone, facsimile, Internet, or e-mail, requires a "known" recipient with a "need to know" the SSI. E-mail attachments containing SSI should be encrypted or password-protected, and the key or password should be provided separately.

Return – The following apply to the CRC Program

- For employees leaving the program, the employee's immediate manager should assure the return of SSI and should brief the exiting employees on their obligation not to disclose SSI. Similarly, employees who transfer to new positions should return SSI records that they no longer need.

- The CRC program shall require contractors, vendors, and suppliers to return SSI at the termination of their contracts or whenever it is no longer needed.

Destruction – The following apply to the CRC Program:

- Paper SSI must be destroyed using a method that precludes its recognition or reconstruction by use of the available 'cross-cut' shredders located in the office.

- Audits or inspections may be done at intervals consistent with the WSDOT's management principles.

Training – The following apply to the CRC Program:

- All program employees who may create, receive, or use SSI should receive training on how to identify, handle, and protect it as part of their training on the PMP and Procedures.

- In addition, SSI awareness training should be included in all new employee and refresher training.

- Contractors, vendors, and suppliers who may need access to SSI as part of their work should also be trained, either by the transit agencies or through their own companies.

3.8 Controlled Documents

Certain key project documents will be classified as "controlled documents." They are documents that are either developed or used during the implementation and management of the CRC Program.

3.8.1 General Controlled Documents Guidelines

The following controlled document guidelines have been established for the CRC Program:

- Each discipline-specific task manager is responsible for identifying Program-specific controlled documents that are either developed internally or acquired from external sources, and require controlled distribution.
- The discipline producing a controlled document is responsible for any necessary updates, approvals, and subsequent redistribution of that controlled document.
- Controlled documents prepared by contractors shall be prepared in accordance with CRC requirements and procedures, and approved or accepted by the responsible discipline specific task managers.

The CRC Program has established a matrix of controlled documents that are subject to controlled distribution. The matrix identifies the discipline-specific Task Leads who are responsible for tracking and updating program-specific controlled documents that are either internally developed documents or externally issued reference documents used in the development of the CRC Program.

3.8.2 Controlled-Distribution Procedure

Many documents will be subject to controlled distribution so that changes and updates are made in a systematic manner, and so that all parties are working on the latest version of the documents. Controlled-distribution procedures involve controlling or regulating the creation, approval, and modifications to key documents that are either developed by the CRC Team or used during the implementation and management of the Program.

Administrative assistants who report to the Highway, Structures, Transit, and Delivery Managers are responsible for coordinating the administration of key documents and records produced internally within their respective discipline and those acquired from external sources and used as authoritative references by CRC staff. Appendix E to the PMP, the *Quality Assurance Manual*, describes in detail the controlled-distribution procedures for internally produced and external reference documents.

3.9 Document Control File Storage Structure (FSS)

The CRC project generally utilizes a standardized electronic file structure and file nomenclature that culminates into an informal file storage structure (FSS). It is important to note the retrievability of electronic files is accomplished through database tracking and full text document searches rather than the nomenclature itself. As such, the document control structure is set up for generalized standardization that is modified as needed to best accommodate the project team.

The structure is a five tiered system as shown below:

3.9.1 Level 1 Program or Project

The first level is implied within the Prolog project name where the file resides as well as the folder structure in which the document resides. Please note: this level is not included in the file name as it would be redundant and would serve no additional purpose. Currently, all project files are included in the CRC Project Files:\ folder which is at a programmatic level rather than a package or project level. Once individual contract packages (projects) are let, the folder structure and database project will reflect this designation at the highest level.

3.9.2 Level 2 Document Type

The second level is included within the prolog project file and the folder structure of where the document resides. It is not included in the file name as it would be redundant. Currently the large categories of file types are: Agreements, Contracts, Visual Library, Deliverables, and Correspondence. Folders levels will be added or merged based on their need.

3.9.3 Level 3 Document ID

Document ID relates to the identifying characteristics of the document type. For Deliverables, the Document ID is the deliverable number assigned in the scope of work. For Correspondence or Public Disclosure documents the document ID corresponds to its unique Prolog ID. For agreements, contracts and pay requests, the document ID corresponds to its agreement or contract number.

3.9.4 Level 4 Year, Month, Day

Level four represents the date of the document in the format Year-Mo-Da. This date is included in the file name immediately following the document ID.

3.9.5 Level 5 Unique ID where Required

In some cases there may be multiple documents that have almost identical file names and need additional clarification. For example, in some instances of Public Disclosure there are multiple entities that receive the exact same request and turn to the project to fulfill the request. In these instances the file name may be followed by a -1, -2 or -3 etc.

3.10 Document Security

To ensure the integrity of project files, the CRC Program has developed permissions that enable users to view, edit, and delete certain documents depending on where these documents are located and what user group the individual is assigned to. The table below summarizes the basic users and their related permissions:

Document Location	Group	Default Permissions
Workpaper Files	All CRC Users	Add, Modify, Delete
Project Files (except DOT folder)	All CRC Users	Read Only
	Administrators, Document Control	Add, Modify, Delete
Project Files DOT Folders	All CRC Users	No Access
	DOT and Management Group	Read Only
	Administrators, Document Control	Add, Modify, Delete
Controlled Documents	All CRC Users	Read Only
	Administrators, Document Control	Add, Modify, Delete
Reference Files	All CRC Users	Read Only
	Administrators, Document Control	Add, Modify, Delete
Document Control In-Box	All CRC Users	Add
	Administrators, Document Control	Add, Modify, Delete

In order to be assigned to a user group, the person must have a CRC network login. Some files that have contents that are not considered to be appropriate for widespread distribution are kept in the Department of Transportation folders.

4. Public Records Laws and Retention

4.1 Public Records Laws

4.1.1 Washington's Public Records Laws

Washington's Public Records Laws are covered under RCW 40.14 and apply to all public entities in the State of Washington.

4.1.2 Oregon's Public Records Laws

Oregon's Public Records Laws are covered under ORS 192 and apply to all public entities in the State of Oregon.

4.1.3 Federal Public Records Laws

Federal records retention requirements may also apply. For instance, records produced in conjunction with a federally funded project would need to be retained as specified in federal laws and regulations and in FTA and FHWA grant requirements.

4.2 Records Retention and Disposition Requirements

All records, regardless of physical form or characteristics that are "made, received, filed or recorded in pursuance of law or in connection with the transaction of public business" must be retained in accordance with the State law.

In addition to state retention requirements, all federally funded projects must comply with retention rules set forth in the Federal Transit Administration and Federal Highway Administration Master Agreements.

CRC will follow the strictest requirement for retention of public records. At the completion of the project, all CRC project office records will be conveyed to the State of Washington in accordance with RCW 40.14.

This page left blank intentionally.

Attachment A-1: Controlled Document List

CRC Controlled Document List

Creating Entity	Controlled Document Name	Owned by (CRC Discipline / Lead Person)
CRC Program	Project Management Plan (PMP)	Business Services / M. Williams
CRC Program	Procedures Manuals	Business Services / M. Williams
CRC Program	Quality Assurance Manual	QA/QC / M. Hohbach
CRC Program	Quality Control Plan	QA/QC / M. Hohbach
CRC Program	Technical Capacity and Capability Plan	Program Manager/ R. Mabey
CRC Program	Project Implementation Plan	Project Delivery / M. Niemi
CRC Program	Real Estate Acquisition Management Plan	Specialty Services / M. Guichard
CRC Program	Safety and Security Management Plan	Transit / G Ficek
CRC Program	Finance Plan	Finance / S. Siegel
CRC Program	Risk and Contingency Management Plan	Project Controls / M Gabel
CRC Program	CRC Design Criteria and Design Deviations / Exceptions	Highway / C. Liles
CRC Program	Final Design Application and Related Documents (Covers Road Map Deliverables)	Transit / G Ficek
CRC Program	New Starts Updates	Transit / K. Betteridge
CRC Program	PE Application / Acceptance Letter	Transit / G Ficek
CRC Program	CRC Transit Design Criteria	Transit / G Ficek

This page left blank intentionally.

Attachment A-2: Front and Back Cover Page for Marking SSI Materials

Appendix A 2

Front and Back Cover Page for Marking SSI Materials

SENSITIVE SECURITY INFORMATION

Columbia River Crossing

Washington Department of Transportation

700 Washington Street – Suite 300

Vancouver, WA 98660

If this document/information is found, please deliver to appropriate department or position as soon as possible.

This page left blank intentionally.

Attachment A-3: TSA's Sensitive Security Information Stakeholder Best Practices Quick Reference Guide

Appendix A 3

Sensitive Security Information Stakeholder Best Practices Quick Reference Guide

What is SSI?

Sensitive Security Information (SSI) is information that, if publicly released, would be detrimental to transportation security as defined by Federal regulation 49 C.F.R. part 1520.

Although SSI is not classified information, there are specific procedures for recognizing, marking, protecting, safely sharing, and destroying SSI.

Recognizing SSI

The following information constitutes SSI:

1. Security programs and contingency plans
2. Security directives
3. Information circulars
4. Performance specifications
5. Vulnerability assessments
6. Security inspections or investigative information
7. Threat information
8. Security measures
9. Security screening information
10. Security training materials
11. Identifying information of certain transportation security personnel
12. Critical infrastructure asset information
13. Systems security information
14. Confidential business information
15. Research and development
16. Other information as determined in writing by the TSA Administrator

The purpose of this brochure is to provide transportation security stakeholders with best practices for handling SSI. Best practices are not to be construed as legally binding requirements of, or official implementing guidance for, the SSI regulation.

The SSI Office

TSA's Sensitive Security Information (SSI) Office:

- ✓ Develops SSI guidance, policies, and procedures to help others appropriately recognize and handle SSI.
- ✓ Analyzes and reviews records for SSI content.
- ✓ Trains TSA employees, clients, and stakeholders in identifying, handling, marking, sharing, storing, transmitting, and destroying SSI.
- ✓ Coordinates with stakeholders, other governmental agencies, and Congress on SSI-related issues.

www.tsa.gov

For more information:

Phone: (571) 227-3513
Fax: (571) 227-2945
SSI@dhs.gov

SENSITIVE SECURITY INFORMATION
SSI
SAFELY SHARING INFORMATION

Sensitive Security Information

✓Stakeholder Best Practices Quick Reference Guide

Transportation Security Administration

Safely Sharing Information

SSI Requirements

The SSI regulation mandates specific and general requirements for handling and protecting SSI.

You Must – Lock-up All SSI
When not in physical possession, store SSI in a secure container such as a locked file cabinet or drawer.

You Must – When No Longer Needed, Destroy SSI
Destruction of SSI must be complete to preclude recognition or reconstruction of the information.

You Must – Mark SSI
The regulation requires that when only a small portion of a paper document contains SSI, every page of the document must be marked with the SSI header and footer shown below.


Sensitive Security Information

[TEXT]

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

When Combining SSI With Other Sensitive But Unclassified (SBU) Information, the document must be marked as SSI. SSI extracted from SSI documents requires the new document to be marked and protected as SSI.

Best Practices Guide

Reasonable Steps Must be Taken to Safeguard SSI. While the regulation does not define reasonable steps, the TSA SSI Office offers these best practices as examples of reasonable steps:

- ✓ **Electronic Presentations** (e.g., PowerPoint) should be marked with the SSI header on all pages and the SSI footer on the first and last pages of the presentation.
- ✓ **Spreadsheets** should be marked with the SSI header on every page and the SSI footer on every page or at the end of the document.
- ✓ **Video and Audio** should be marked with the SSI header and footer on the protective cover when able and the header and footer should be shown and/or read at the beginning and end of the program.
- ✓ **CDs and DVDs** should be encrypted or password-protected and the header and footer should be affixed to the CD or DVD.
- ✓ **Portable Drives** including "flash" or "thumb" drives should not themselves be marked, but the drive itself should be encrypted or all documents stored should be password-protected.
- ✓ **When Leaving Your Computer or Desk** you must lock up all SSI and should lock or turn off your computer.
- ✓ **Taking SSI Home** is not recommended, but if necessary, get permission from a supervisor and lock up all SSI at home.
- ✓ **Discussing SSI Over Cellular Telephones** should be done carefully to prevent eavesdropping. Land lines in non-public locations are more secure than cellular telephones.
- ✓ **Email** should not contain SSI in the body of the email. SSI should be emailed in a password-protected attachment. Passwords should be sent separately with no subject line or shared either in person or via telephone.
- ✓ **Passwords for SSI Documents** should contain at least 8 characters, have at least one upper-cased and one lower-cased letter, contain at least one number, and not be a word in the dictionary.
- ✓ **Faxing of SSI** should be done by first verifying the fax number and that the intended recipient will be available to retrieve the SSI once faxed.
- ✓ **SSI Should Be Mailed** by U.S. First Class mail or other traceable delivery service using an opaque envelope or wrapping and the outside wrapping should not be marked as SSI.
- ✓ **Interoffice Mail** should be sent using an unmarked, opaque, sealed envelope so that the SSI cannot be read through the envelope.
- ✓ **SSI Stored on Network Folders** should either require a password to open or the network should limit access to the folder.
- ✓ **Destroying SSI** should be done using a cross-cut shredder which produces particles that are 1 ½ inch by ¾ inch or smaller.

Sensitive Security Information Office

Safely Sharing Information

This page left blank intentionally.

Attachment A-4: NDA Log

CRC Project NDA Repository Log
_____ Team

			Examined Documents							Repository Document (Retained)									
										Location A: _____		Location B: _____		Location C: _____		Location D: _____		Location E: _____	
ID	Date Viewed/ Retained	NDA Protected Party	Document Type	Document Date	Identifying Characteristics	Document Subject	Logged By	Total Pages Viewed	Total Pages Retained	Date Placed	Date Destroyed	Date Placed	Date Destroyed	Date Placed	Date Destroyed	Date Placed	Date Destroyed	Date Placed	Date Destroyed
1	2	3	4	5	6	7	8	9	10										

This page left blank intentionally.

Attachment A-5: NDA ID Form

CRC NDA Document ID

Note: Fill out this form for each examined document.

Unique Doc ID * _____ **Date Viewed** _____

NDA Team Name _____ **NDA Protected Party** _____

Document Description

Type: Letter ☐ Drawing ☐ Mtg Minutes ☐

Memo ☐ Report ☐ Other _____

Atrributes:

Document Date _____

Identifiying Characteristics _____

Subject _____

Other _____

Total # of Pages Viewed _____

Total # of Pages Retained _____

Team Members Viewing: _____ _____ _____ _____

Delivered By _____ **Signature** _____

Logged By _____ **Signature** _____

Provide Additional Notes If Needed Below :

* Unique ID is assigned by PW Adminstrator

This page left blank intentionally.