A Project Document of the ATC Cybersecurity Project

Cybersecurity for the Advanced Transportation Controller (ATC) Standards PMP v01.06

Project Management Plan (PMP) for the Cybersecurity for Advanced Transportation Controller (ATC) Standards Family Project

November 21, 2022

PMP in support of:	USDOT Contract # FHWA 693JJ321D000005 Task Order # 693JJ321F000419
For approval by:	Steve Sill, ITS Architecture & Standards Program Manager USDOT ITS Joint Program Office
For use by:	Siva Narla, Senior Director, Transportation Technology Institute of Transportation Engineers ATC Program Manager Nicola Tavares, Technical Products Manager Institute of Transportation Engineers Project Manager for the ATC Cybersecurity Project Ralph W. Boaz, President Pillar Consulting, Inc. Technical Lead for the ATC Cybersecurity Project Members of the Infrastructure Security Committee Project Team for the ATC Cybersecurity Project
Prepared by:	Ralph W. Boaz Siva Narla

CHANGE HISTORY

Version	Date	Editor	Notes
v01.06	11/21/22	Boaz	Changes to address a change in scope. The project to include the addition of a Threat Analysis as part of the Concept of Operations. Replaced Infrastructure Security Committee (ISC) with Steering Committee or SC. Updated Figure 6 graphic.
v01.05	04/17/22	Boaz	Changed "security" to "cybersecurity" to be consistent with changes in v01.03. Added Keith Wilson as SAE Liaison.
v01.04	03/31/22	Boaz	Updated schedule per USDOT.
v01.03	03/23/22	Boaz / Madineni	Changed name of standard to ATC Cybersecurity Standard. Added project schedule. Made other text modifications. Updated appendix and reference section.
v01.02	03/02/22	Boaz	Changed project to create an ISC Security Standard.
v01.01	02/12/22	Boaz	Interim draft for review by the SME team.
v01.00	10/25/21	Narla	Initial Draft for this Project Management Plan (PMP) v01.00.

CONTENTS

TABLE OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 Purpose of the Project Management Plan

This document defines a Project Management Plan (PMP) for the Cybersecurity for the Advanced Transportation Controller (ATC) Standards Project under the United States Department of Transportation (USDOT) Contract # DTFH61-16-D-00055, Work Order # 19-0403. This PMP identifies the activities for the project and establishes a common understanding for the management of the project for:

a) The USDOT Intelligent Transportation Systems (ITS) Joint Program Office (JPO) who is sponsoring the work.

b) The partner Standard Development Organizations (SDOs) who are representing stakeholders for this project.

c) The project team contracted to perform the work.

d) The ATC Cybersecurity Steering Committee (Steering Committee or SC) as the oversight group to develop standards relevant to cybersecurity of ATC standards under this task.

e) The broad stakeholder community made up of infrastructure, cybersecurity and connected vehicle communities represented by AASHTO, NEMA, SAE, ITE and others.

This PMP is based on the Performance Work Statement (PWS) for the "Cybersecurity for the Advanced Transportation Controller" project provided by the USDOT. The PMP includes plans for scope management; communications; deliverables and milestones; quality management; human resource management; and a Systems Engineering Management Plan (SEMP). Portions of this PMP may be updated during the course of the project if the Project Management Team (PMT) or the USDOT determines that modification would significantly facilitate the project management functions. The PMP is not intended to be a progress tracking tool or to be modified for minor changes in schedule once the project has started.

This project addresses cybersecurity for ATC field equipment including access control to the cabinet in order to defend against unauthorized entry. For convenience and consistency with the formal project title, the project is referred to as the "ATC Cybersecurity Project."

1.2 Background of Project

USDOT and ITE and their standards development partners, AASHTO and NEMA, have developed and published ITS standards since the inception of the ITS Standards Program over 25 years ago. Between 1998 and 2016, ITE led the SDO team with AASHTO and NEMA for the development of ATC standards to support Intelligent Transportation Systems. AASHTO serves its member departments, the USDOT, and Congress, by providing leadership, technical services, information, and advice as well as contributing to national policy on transportation issues. NEMA is the trade association of choice for the electrical manufacturing industry with 430 member companies manufacturing products used in the generation, transmission and distribution, control, and use of electricity. ITE's team served as the organizational and administrative bureau for the ATC Joint Committee. Beginning in 2016, the overall contract to develop and maintain ATC standards is under a single contract, with ITE being the prime contractor, and AASHTO, NEMA, and subject matter experts (SME's) serving as subcontractors. This maintenance task is to be executed within the scope of the overall contract.

The USDOT has supported development of ATC family of standards including: the Advanced Transportation Controller (ATC) 5201 v06A Controller Standard, the ATC 5401 Standard v02A Application Programming Interface (API) for the Advanced Transportation Controller Standard, and the ATC 5301 v02 ATC Cabinet Standard for over 20 years. Development of these standards has been accomplished by the cooperative and volunteer efforts of the private and public sector members of the ATC working groups (WGs): the Controller WG, the API WG and the Cabinet WG. The infrastructure community has lent its support in the development of these ATC family of standards as they are critically important to the deployment of ITS systems that are interoperable and sustainable nationwide. The deployment of connected vehicle (CV) technologies has brought urgency to the need for heightened cybersecurity on ITS infrastructure devices and it is driving changes to the ATC standards to ensure connected infrastructure readiness.

The need to develop user needs, system requirements and design, specifically to address cybersecurity related features, has been identified across all three of the ATC standards while undergoing periodic maintenance and during recent maintenance activities. This level of development is beyond that of typical maintenance activities and requires a formal standards development effort that employs a full systems engineering process.

ITE, with support from NEMA, AASHTO, SAE and other organizations, will develop a cybersecurity standard consistent with ATC standards family to help increase the cybersecurity of ITS infrastructure deployments nationwide. The project will use a systems engineering process, cybersecurity principles, and a standards development process to produce interim and final deliverables as identified in Section 2.2.1 Scope Statement and in Table 4.

ITE will engage a broad base of stakeholders including members from the Roadway Transportation System Cybersecurity Framework (RTSCF) project working groups; the ATC Joint Committee and its working groups; and the NTCIP Joint Committee and its working groups. ITE will also consult with SAE and its technical committees as well as other cybersecurity research and testing communities. ITE will leverage recent Connected Vehicle efforts such as the RSU Standards Working Group, Connected Intersections (CI) Committee and its Security Task Force, and the Cooperative Automated Transportation (CAT) Coalition. ATC standards are jointly published by the American Association of State Highway and Transportation Officials (AASHTO), National Electrical Manufacturers Association (NEMA), and ITE, per these associations' existing agreement.

ITE will establish the Steering Committee as the oversight group (similar to the ATC Joint Committee) supporting this standards development effort. The Steering Committee will comprise of voting members from relevant stakeholder communities. Although there are voting members identified, attendance to the proceedings of the Steering Committee will be open to all members, stakeholders and interested parties. In addition, representatives of cybersecurity agencies or researchers may be invited with prior approval of USDOT Contracting Officer’s Representative.

This project has four major objectives:

1) Establish a stakeholder group with balanced representation from both current infrastructure as well as the Connected environment that is focused on cybersecurity of all deployments based on the ATC standards (published and currently in ballot).
2) Ensure broad outreach to infrastructure, cybersecurity and connected vehicle communities represented by AASHTO, NEMA, SAE, ITE and other organizations. With the help of stakeholders, create a set of cybersecurity needs, requirements and design through a systems engineering process.
3) Build a cybersecurity standard for the ATC family that is deployable and sustainable nationwide. This cybersecurity standard could also be applicable to other infrastructure and CV systems.
4) Publish cybersecurity updates to the ATC standards that ensures resiliency, using the systems engineering and SDO processes.

ITE as an SDO provides this service through a process which is adapted from the American National Standards Institute’s (ANSI) process for developing standards and is approved by the ITE Board of Direction. The process is based on fair and open participation of stakeholders from the public and private sector and practitioners with valuable support from the USDOT. ITE’s SDO process coupled with MOUs with other SDOs identifies ITE's approach to addressing the standard development task order for the cybersecurity standard for the ATC standards family.

ITE has implemented organizational and participatory structures and processes to promote interaction among interested parties for Institute standards as well as ITS Standards. The procedures are designed to ensure compliance with required standards-making processes and provide the necessary documentation to address any inquiries or noted problems. The intended objective of these procedures for the development of Institute standards is to ensure procedural fairness to all interested parties, through a coordinated effort with reasonable safeguards to guard against any potential harmful effects of standards and realistic appeals procedures.

The procedure for standards development is generally outlined as in the following steps. Once a decision is made to develop an ITE Standard or Recommended Practice, a committee is assigned the preparation task. The draft material is subjected to a review process before the proposed standard is published. A list of persons interested in the standard is maintained, and these persons are kept up to date on the development of the standard. Notices are also published by ITE notifying interested parties of the status of specific standards. All comments and input received on proposed standards are addressed prior to final adoption. An appeals process is provided to resolve any final disagreements on a specific standard or to address the standards development procedures.

ITE may hold face-to-face meetings to conduct walkthroughs of the Concept of Operations (see Section 2.2.1.2.3), the System Requirements Specification (see Section 2.2.1.3.2), and the System Design Description (see Section 2.2.1.4.2). These walkthroughs are open to everyone. Public sector members of the Steering Committee, the SMEs on the project team (PT), and SDO representatives are proposed to be reimbursed for their travel with prior approval of the ATC Cybersecurity Project Manager (PM). The Steering Committee is to be comprised of 16 members (7 public and 9 private sector members are proposed). Total personnel needing reimbursement are then estimated to be seven public sector representatives, four SDO representatives, and five SME's for a total of 16 person trips for each walkthrough. The total estimated trips are then estimated to be forty-eight (48) for three walkthroughs.

2 SCOPE MANAGEMENT PLAN

2.1 Purpose of the Scope Management Plan

This Scope Management Plan establishes the scope management approach and processes as they pertain to scope description, verification, and control measures for the project. It establishes the processes which ensure that the ATC Cybersecurity Project includes all of the tasks required to complete the work identified while excluding all work that is unnecessary.

2.2 Scope Statement

2.2.1 Project Scope Description

The subsections below describe the project activities listed in the Gantt Chart in Section 4.3 Project Schedule. The development of the deliverable documents is conducted using a cyclical draft-review-update process with qualified reviewers in the ATC WGs and Steering Committee that are not a part of the subconsultant team. Each of the major project tasks are listed below with the objectives, approach, and deliverables identified. ITE will provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform the tasks. Tasks specifically identified in the PWS are identified in brackets with the PWS task number (i.e. [PWS Task #]). Specific deliverables identified in the PWS are identified in brackets as "[PWS Deliverable]."

The project develops an ATC Cybersecurity Standard from which needs and requirements may be referenced in the ATC standards ATC 5201, ATC 5401, and ATC 5301. Some design details may be included in the ATC Cybersecurity Standard while other design details may be developed by the ATC standards working groups for the various ATC standards. The primary activity of this project scope description is the development of the ATC Cybersecurity Standard (Tasks 1-5, Sections 2.2.1.1-2.2.1.5). The subsequent tasks of ATC Cybersecurity Standard verification and validation (Task 6, Section 2.2.1.6) and updates to the ATC standards (Task 7, Section 2.2.1.7) may be modified based on project developments.

2.2.1.1 Task 1 Project Management [PWS Task 1]

The purpose of this task is for ITE to establish the management processes for the ATC Cybersecurity Project. The project management activities include the development of a Project Management Plan (PMP) and Systems EngineeringManagement Plan (SEMP). The following stipulations apply:

- The approved version of the PMP, SEMP and project schedule will only be modified with pre-approval from the Contracting Officer's Representative (COR) and any modified version will be delivered to the COR within 10 working days after receiving COR approval.
- Once the draft PMP, SEMP and project schedule are ready for review, a meeting with the USDOT and its representatives will be scheduled to review each document and ensure that all parties are in agreement on the overall approach to project execution.
- The revised version of each contract deliverable (including the detailed project schedule) will be under document configuration control with version numbers assigned to each document. All documents submitted to and approved by the USDOT will be assigned a unique version number.
- An authorization to proceed (ATP) is pursuant to USDOT's approval of a revised PMP and schedule.

2.2.1.1.1 Task 1.1 Kick-off Meeting [PWS Task 1.1]

Objectives

- ITE and ITE's subcontractors will participate in a "kick-off" meeting with the USDOT and its representatives to ensure that all parties have a clear understanding of the requirements of this PWS and what are the USDOT's expectations.
- The kick-off meeting will take place within 30 working days of the effective date of the task order unless otherwise agreed to by the Government.

Approach

- At the kick-off meeting, the ITE will provide a draft PMP/SEMP and a detailed project schedule in Microsoft Project format that lists all milestones. The Project Schedule will address all project management and engineering activities.
- ITE will provide an updated Project Schedule, reflecting actual work performed, with every Monthly Progress Report (MPR) that it submits. The monthly updated project schedule will reflect both the base-lined task start and end dates and the actual start and end dates for each task in the Project Schedule. The project schedule will be provided in both Microsoft Project and Adobe Acrobat formats. See Section 2.2.1.1.3 Monthly Reporting and Section 4.1 Monthly Progress Reports.

Deliverables

- None. Draft versions of the deliverables in Task 1.2 will be used.

2.2.1.1.2 Task 1.2 Project Management Plan and Systems Engineering Management Plan [PWS Task 1.2]

Objectives

- ITE will develop a Project Management Plan (PMP) that includes the activities defined for a Systems Engineering Management Plan (SEMP).

Approach

- ITE will develop a Draft PMP.
- The PMP describes the overall approach to managing the efforts described in the PWS and coordinating the work performed by all subcontractors.
- The PMP will describe the overall structure of the ITE team; explain the roles and responsibilities of all key individuals (including infrastructure owner operator, device vendor, cybersecurity, radio, and wireless communications experts); and describe the reporting relationships among the team.
- The PMP will contain a Human Resources Management Plan (or Team Management Plan) that includes team resumes, representing domain experts and a qualified technical editor. The Human Resources Management Plan, including project team members, is subject to USDOT approval as part of the overall approval of the PMP.
- ITE will describe its Quality Management and how it will ensure that the documents submitted as deliverables herein, will:
  - Contain suitable material for the target audience;
  - Be organized in presentation;
  - Contain proper word use and English diction;
  - Contain detailed illustrations;
  - Be comprehensive, complete, and correct; and
  - Be edited for grammatical and editorial errors.
- The Quality Management section is subject to USDOT approval as part of the overall approval of the PMP. ITE will describe how they will coordinate their efforts with the USDOT, particularly the Task Order Contracting Officer's Representative (TOCOR) and the Contracting Officer (CO).
- ITE will describe how they will work with SAE to develop and review all major sections of the standard.
- ITE will prepare a detailed project schedule, in Microsoft Project format, that lists all planned tasks and milestones for the project. The detailed project schedule will reflect a work breakdown structure (WBS) comprised of at least three levels. ITE will provide an updated Project Schedule, reflecting actual work performed, with every Monthly Progress Report that it submits (see below for report content and scheduled delivery dates). The monthly updated Project Schedule will reflect both the baselined task start and end dates and the actual start and end dates for each task in the Project Schedule.
- The PMP will include activities associated with an SEMP. ISO/IEC/IEEE 24748-4-2016 will be used for guidance in this area. Activities associated with the SEMP will be clearly distinguishable from other project activities.
- The SEMP activities will also include the following sections: a Configuration Management Plan, Verification and Validation Plan, and a Risk Management Plan.
- ITE will revise the final approved version of the PMP and SEMP only with pre-approval from the COR and will deliver, to the COR, any modified version within 10 working days after receiving COR approval.
- ITE will put the revised version of each contract deliverable (including the detailed project schedule) under document configuration control, with version numbers assigned to each document. All documents submitted to, and approved by, USDOT will be assigned a unique version number.
- ITE will deliver a monthly progress report.

Deliverables

- Draft PMP with SEMP and Project Schedule [PWS Deliverable]
- PMP with SEMP and Project Schedule [PWS Deliverable]

2.2.1.1.3 Task 1.3 Monthly Progress Reporting

Objectives

- Establish and execute the process of monthly project reviews.

Approach

- Prepare and deliver monthly progress reports for the ATC Cybersecurity Project as defined in Section 2.2.1.1.1 Kick-off Meeting and Section 4.1 Monthly Progress Reports.

Deliverables

- Monthly Progress Reports [PWS Deliverable]

2.2.1.2 Task 2 Develop Concepts of Operations (ConOps) for the ATC Cybersecurity Standard [PWS Task 2]

The purpose of this task is to develop a Concept of Operations (ConOps) for the ATC Cybersecurity Standard.

2.2.1.2.1 Task 2.1 Review Relevant Prior and Ongoing Research

Objectives

- Review Relevant Prior and Ongoing Research related to projects associated with the standard under development/update and gain a clear understanding of the prior work.

Approach

- ITE will review ongoing and prior research related to projects including cybersecurity for ITS field devices to gain a clear understanding of the prior work. ITE will become conversant with the research activities in the relevant areas and assess the potential impact that relevant projects (e.g., CV Pilots and Smart Cities) may have on the output of this project. In addition, other standards such as the CI Implementation Guide, NIST Special Publication 800-82r2, NIST Special Publication 800-53, NIST Special Publication 800-63B, CIS Controls Version 7 Implementation Guidance for Industrial Control Systems, the NIST Cybersecurity Framework for Connected Vehicle Environments, the NIST Framework for Improving Critical Infrastructure Cybersecurity, and the ITS Architecture Cybersecurity Analysis should be reviewed for relevant user needs and use cases. A white paper identifying key sources and summarizing the findings of this early research will be created as a deliverable using the following resources as guidance
  - ISO/IEC/IEEE 15288:2015 and/or ISO/IEC/IEEE 15288 AWI
  - NIST SP800-160 volume 1 and volume 2
  - https://attack.mitre.org/
  - https://collaborate.mitre.org/attackics/index.php/Main_Page
  - Investigate available secure software development frameworks for software cybersecurity processes and identify one or more appropriate approaches suitable for adoption or adaption to apply to the remainder of task activities.
- The USDOT will review and provide comment on the white paper. ITE will modify the white paper based on the USDOT comments.
- ITE will interview key stakeholders as part of the research. The stakeholders will include ATC equipment vendors, infrastructure owner operators (IOOs) and cybersecurity subject matter experts. Preferably the equipment vendors and IOO stakeholders will have a level of cybersecurity knowledge and how cybersecurity is currently addressed in the equipment/systems.

A stakeholder list will be developed by ITE and must be approved by USDOT prior to conducting the interviews.

- ITE will develop a questionnaire to be used during stakeholder interviews. ITE will deliver a draft version of the questionnaire to USDOT for review and comment. ITE will modify the questionnaire within 10 working days of receiving comments from the USDOT. After the questionnaire is approved by the USDOT, it will be used by ITE in the stakeholder interviews
- ITE will perform the stakeholder interviews and create a summary report for the USDOT to review and comment. The stakeholder summary will be updated based on USDOT comments.

Deliverables

- Stakeholder and Subject Matter Expert List [PWS Deliverable]
- Draft Stakeholder Interview Questionnaire [PWS Deliverable]
- Stakeholder Interview Questionnaire [PWS Deliverable]
- Draft Stakeholder Interview Summary Report
- Stakeholder Interview Summary Report [PWS Deliverable]
- Draft White Paper Summarizing Sources and Research [PWS Deliverable]
- White Paper Summarizing Sources and Research [PWS Deliverable]

2.2.1.2.2 Task 2.2 Develop Draft ConOps for the ATC Cybersecurity Standard

Objectives

- Develop a draft ConOps for the developing standard.

Approach

- ITE will develop a draft ConOps for the ATC Cybersecurity Standard with guidance of ISO/IEC/IEEE 29148:2011 and NTCIP 8002 Annex B1. See the PWS, Appendix B, Section 2 for an example outline.
- ITE will develop the user needs for the ConOps. They will be derived from the research and interview activities defined in the previous subtasks.
- The user needs will be well-written as described in the PWS, Appendix A.
- The user needs will be in accordance with cybersecurity best practices, supportable by the IOO community within their larger cybersecurity processes and lean on the principles of good cybersecurity for industrial control systems.
- The user needs will describe expected technical, environmental, and institutional constraints for the system of interest. These items will provide system concepts (including a high-level discussion of technical and non-technical requirements), operational scenarios, and the rationale for key concept decisions.
- ITE will develop a context diagram as part of the ConOps that shows the environment the device will work in and any possible options in the high-level architecture.
- ITE will perform a cyber threat analysis that investigates potential attack scenarios against ATC equipment and systems.
- The threat analysis will be documented using an attack tree form and identify proposed mitigations. New user needs discovered during the threat analysis will be added to the ConOps.
- ITE will deliver a draft version of the ConOps to the Steering Committee, ATC WGs, and USDOT to be used during the walkthrough.

Deliverables

- Draft ConOps [PWS Deliverable]

2.2.1.2.3 Task 2.3 Walkthrough on Draft ConOps

Objectives

- Prepare and perform a walkthrough of the Draft ConOps.

Approach

- In consultation with the COR, ITE will prepare a list of knowledgeable SMEs from industry stakeholders (e.g., USDOT, state and local transportation agencies, center-to-field experts, car manufacturers, transit operators, commercial vehicle operations (CVO) operators, contractors involved with ITS research; telecommunications experts, transportations service industry; other public sector representatives, and relevant other Standards Development Organizations and/or working groups) in order to invite them to attend a face-to-face review of the draft ConOps.
- The SMEs will provide comments on the ConOps from a functional, technical, management and implementation perspective.
- In consultation with the COR, ITE will arrange for a time and facility (virtual, hybrid, or in-person as appropriate) where the walkthrough will take place. ITE will be responsible for invitations, distributing advance material including the draft ConOps, registrations, travel reimbursement, note taking, and coordination of the walkthrough.
- IEEE Std 1028-2008 will be used for guidance in planning the walkthrough.
- A ConOps Walkthrough Plan will be prepared and provided to USDOT for approval at least 30 days prior to the scheduled walkthrough.
- ITE will prepare and distribute a Walkthrough Workbook to be used to guide the walkthrough. It will be sent to stakeholders at least 10 working days prior to the walkthrough.
- ITE will deliver a ”Walkthrough Comment Resolution” report which details each walkthrough comment and ITE’s recommended resolution.

Deliverables

- Draft ConOps Walkthrough Plan [PWS Deliverable]
- ConOps Walkthrough Plan [PWS Deliverable]
- ConOps Walkthrough Workbook [PWS Deliverable]
- ConOps Walkthrough Comment Resolution Report [PWS Deliverable]

2.2.1.2.4 Task 2.4 Develop Final ConOps

Objectives

- Develop the final ConOps for the developing standard.

Approach

- Develop the final ConOps document incorporating the walkthrough comment resolutions.
- The ConOps will be considered a “living” document (i.e., one that may be modified as needed during the development of the standard).
- ITE will put the “final” version of each contract deliverable under document configuration control with version numbers assigned to each document.
- If a document considered “final” undergoes subsequent revision, it will be checked out of the document configuration control system and checked back in once a new “final” version is accepted by the Steering Committee.

Deliverables

- ConOps for ATC Cybersecurity Standard [PWS Deliverable]

2.2.1.3 Task 3 Develop System Requirements Specification (SRS) for the ATC Cybersecurity Standard [PWS Task 3]

The purpose of this task is to develop a System Requirements Specification (SRS) for the ATC Cybersecurity Standard.

2.2.1.3.1 Task 3.1 Develop Draft SRS for the ATC Cybersecurity Standard

Objectives

- Develop a Draft SRS for the developing standard.

Approach

- ITE will develop a draft SRS document based on the ConOps, following the guidance of ISO/IEC/IEEE 29148:2011. A tailored outline, based on ISO/IEC/IEEE 29148:2011, for the requirements section is proposed in Appendix B Section 3 of the PWS.
- The requirements will be mapped from needs identified in the ConOps to requirements in a Needs-to-Requirements traceability matrix.
- The requirements documented in the SRS will meet the test of being “well-formed” requirements. See Appendix A of the PWS for the definition of a “well-formed” requirement
- ITE will review other relevant standards such as the CI Implementation Guide, NIST Special Publication 800-82r2, NIST Special Publication 800-53, NIST Special Publication 800-63B, CIS Controls Version 7 Implementation Guidance for Industrial Control Systems, the NIST Cybersecurity Framework for Connected Vehicle Environments, the NIST Framework for Improving Critical Infrastructure Cybersecurity, and the ITS Architecture Cybersecurity Analysis for suitable cybersecurity requirements.
- ITE will deliver a draft version of the SRS to the Steering Committee, ATC WGs, and USDOT to be used during the walkthrough.

Deliverables

- Draft SRS [PWS Deliverable]

2.2.1.3.2 Task 3.2 Walkthrough on Draft SRS

Objectives

- Prepare and perform a walkthrough of the Draft SRS.

Approach

- In consultation with the COR, ITE will prepare a list of knowledgeable SMEs from industry stakeholders (e.g., USDOT, state and local transportation agencies, center-to-field experts, car manufacturers, transit operators, commercial vehicle operations (CVO) operators, contractors involved with ITS research; telecommunications experts, transportations service industry; other public sector representatives, and relevant other Standards Development Organizations and/or working groups) in order to invite them to attend a face-to-face review of the draft SRS. Where possible, these vendors and IOO representatives will be knowledgeable in cybersecurity and how it is applied in their organizations.
- The SMEs will provide comments on the requirements from a functional, technical, management and implementation perspective
- In consultation with the COR, ITE will arrange for a time and facility (virtual, hybrid, or in-person as appropriate) where the walkthrough will take place. ITE will be responsible for invitations, distributing advance material including the draft ConOps, registrations, travel reimbursement, note taking, and coordination of the walkthrough.
- IEEE Std 1028-2008 will be used for guidance in planning the walkthrough.
- An SRS Walkthrough Plan will be prepared and provided to USDOT for approval at least 30 days prior to the scheduled walkthrough.
- ITE will prepare and distribute a Walkthrough Workbook to be used to guide the walkthrough. It will be sent to stakeholders at least 10 working days prior to the walkthrough.
- ITE will deliver a ”Walkthrough Comment Resolution” report which details each walkthrough comment and ITE’s recommended resolution within 10 working days after the completion of the SRS Walkthrough.

Deliverables

- Draft SRS Walkthrough Plan [PWS Deliverable]
- SRS Walkthrough Plan [PWS Deliverable]
- SRS Walkthrough Workbook [PWS Deliverable]
- SRS Walkthrough Comment Resolution Report [PWS Deliverable]

2.2.1.3.3 Task 3.3 Develop Final SRS

Objectives

- Develop the final SRS for the developing standard.

Approach

- Develop the final SRS document incorporating the walkthrough comment resolutions.
- The SRS will be considered a "living" document (i.e., one that may be modified as needed during the development of the standard).
- ITE will put the "final" version of each contract deliverable under document configuration control with version numbers assigned to each document.
- If a document considered "final" undergoes subsequent revision, it will be checked out of the document configuration control system and checked back in once a new "final" version is approved by the USDOT.

Deliverables

- SRS for ATC Cybersecurity Standard [PWS Deliverable]

2.2.1.4 Task 4 Develop System Design Description (SDD) for the ATC Cybersecurity Standard [PWS Task 4]

The purpose of this task is to develop a System Design Description (SDD) for the ATC Cybersecurity Standard.

2.2.1.4.1 Task 4.1 Develop Draft SDD for the ATC Cybersecurity Standard

Objectives

- Develop a Draft SDD for the developing standard.

Approach

- ITE will develop a Draft SDD based on the ConOps and SRS. IEEE Std 1016-2009 will be used for guidance in this area. An outline is proposed as part of Appendix B of the PWS.
- ITE will document the design solution for each requirement developed in the previous tasks. The SDD will specify the content, constraints and other factors needed to implement cybersecurity for the ATC standards.
- ITE will include a Requirements Traceability Matrix (RTM) in the SDD. The RTM is a table that provides a mapping from each requirement to its associated design content. ITE will use NTCIP 8002 Annex B1 as a guide.
- The system design elements will be in accordance with cybersecurity best practices, supportable by the IOO community within their larger cybersecurity processes and lean on the principles of good cybersecurity for industrial control systems
- ITE will review other relevant standards such as the CI Implementation Guide, NIST Special Publication 800-82r2, NIST Special Publication 800-53, NIST Special Publication 800-63B, CIS Controls Version 7 Implementation Guidance for Industrial Control Systems, the NIST Cybersecurity Framework for Connected Vehicle Environments, the NIST Framework for Improving Critical Infrastructure Cybersecurity, and the ITS Architecture Cybersecurity Analysis for suitable cybersecurity designs.

- Deliver a draft version of the SRS to the Steering Committee, ATC WGs, and USDOT to be used during the walkthrough.

Deliverables

- Draft SDD [PWS Deliverable]

2.2.1.4.2 Task 4.2 Walkthrough on Draft SDD

Objectives

- Prepare and perform a walkthrough of the Draft SDD.

Approach

- In consultation with the COR, ITE will prepare a list of knowledgeable SMEs from industry stakeholders (e.g., USDOT, state and local transportation agencies, center-to-field experts, car manufacturers, transit operators, commercial vehicle operations (CVO) operators, contractors involved with ITS research; telecommunications experts, transportations service industry; other public sector representatives, and relevant other Standards Development Organizations and/or working groups) in order to invite them to attend a face-to-face review of the draft SDD. Where possible, these vendors and IOO representatives will be knowledgeable in cybersecurity and how it is applied in their organizations. ITE will submit the stakeholder list to USDOT for approval prior to organizing the SDD Walkthrough.
- The SMEs will provide comments on the SDD from a functional, technical, management and implementation perspective.
- In consultation with the COR, ITE will arrange for a time and facility (virtual, hybrid, or in-person as appropriate) where the walkthrough will take place. Also, send invitations, distribute advance material including the draft SDD, registrations, travel reimbursement, note taking, and coordination of the walkthrough.
- IEEE Std 1028-2008 will be used for guidance in planning the walkthrough.
- An SDD Walkthrough Plan will be prepared and provided to USDOT for approval at least 30 days prior to the scheduled walkthrough.
- ITE will prepare and distribute a Walkthrough Workbook to be used to guide the walkthrough. It will be sent to stakeholders at least 10 working days prior to the walkthrough.
- ITE will deliver a ”Walkthrough Comment Resolution” report which details each walkthrough comment and ITE’s recommended resolution within 10 working days after the completion of the SDD Walkthrough.

Deliverables

- Draft SDD Walkthrough Plan [PWS Deliverable]
- SDD Walkthrough Plan [PWS Deliverable]
- SDD Walkthrough Workbook [PWS Deliverable]
- SDD Walkthrough Comment Resolution Report [PWS Deliverable]

2.2.1.4.3 Task 4.3 Develop Final SDD

Objectives

- Develop the final SSD for the developing standard.

Approach

- Develop the final SDD document incorporating the walkthrough comment resolutions.
- The SDD will be considered a “living” document (i.e., one that may be modified as needed).
- ITE will put the “final” version of each contract deliverable under document configuration control with version numbers assigned to each document.
- If a document considered “final” undergoes subsequent revision, it will be checked out of the

document configuration control system and checked back in once a new “final” version is approved by the USDOT.

Deliverables

- SDD for ATC Cybersecurity Standard [PWS Deliverable]

2.2.1.5 Task 5 Complete ATC Cybersecurity Standard

2.2.1.5.1 Task 5.1 Develop User Comment Draft (UCD) ATC Cybersecurity Standard

Objectives

- Develop a User Comment Draft ATC Cybersecurity Standard.
- Solicit comments from the distribution of the UCD the SDOs and the transportation industry at large.
- Capture and adjudicate the comments received.

Approach

- Develop a proposed UCD (pUCD) ATC Cybersecurity Standard and submit it to the ATC JC for acceptance.
- Guidance from NTCIP 8002 Annex B1 can be used for guidance.
- Resolve any issues from the ATC JC and gain acceptance of the ATC Cybersecurity Standard.
- Prepare a Standard Development Report (SDR) to accompany the UCD.
- Distribute the UCD though the SDOs for review and comment.
- The ATC WGs adjudicate the comments and come to a consensus on the updates to the UCD that are to be performed.
- Distribute the adjudicated comments in a Comment Disposition Report.

Deliverables

- UCD ATC Cybersecurity Standard
- SDR for ATC Cybersecurity Standard
- UCD Comments Disposition Report

2.2.1.5.2 Task 5.2 Develop Recommended Standard (RS) ATC Cybersecurity Standard

Objectives

- Develop a Recommended Standard (RS) ATC Cybersecurity Standard.

Approach

- Develop a proposed RS (pRS) ATC Cybersecurity Standard based on the Comment Disposition Report and submit it to the Steering Committee for acceptance.
- Resolve any issues from the Steering Committee and gain acceptance of RS ATC Cybersecurity Standard.
- Prepare a Standard Development Report (SDR) and Notice of Intent (NOI) to accompany the RS.
- Distribute the RS though the SDOs for formal ballot.

Deliverables

- RS ATC Cybersecurity Standard
- SDR for RS ATC Cybersecurity Standard
- NOI for RS ATC Cybersecurity Standard

2.2.1.5.3 Task 5.3 Approve ATC Cybersecurity Standard

Objectives

- Develop a Jointly Approved ATC Cybersecurity Standard.

Approach

- Adjudicate and address comments received for the SDO Ballot and NOI period.
- Prepare Comment Disposition Report
- Prepare Jointly Approved ATC Cybersecurity Standard
- Publish Standard.

Deliverables

- Jointly Approved ATC Cybersecurity Standard.

2.2.1.6 Task 6 Develop and Perform ATC Cybersecurity Standard Verification and Validation [PWS Task 5]

Objectives

- Develop a test plan consisting of test cases and test procedures to verify and validate the updates to ATC 5201, ATC 5301 and ATC 5401

Approach

- The test plan, test cases and test procedures will be developed, reviewed and approved within the ATC WGs. The test plan will include full traceability between the new cybersecurity requirements and test cases within each of the ATC standards.
- Work with the ATC stakeholder community to identify vendors and IOOs willing to participate in ATC Cybersecurity Standard verification and validation testing.
- This testing will be accomplished in accordance with the approved ATC Cybersecurity Standard test plan, test cases and test procedures.
- Develop a test report and provide the detailed execution results, defects found, and any issues that may require changes to one or more of the ATC standards.

Deliverables

- ATC Cybersecurity Standard Test Plan [PWS Deliverable]
- ATC Cybersecurity Test Report [PWS Deliverable]

2.2.1.7 Task 7 Update ATC Standards [PWS Task 6]

The purpose of this task is to develop the following standards ATC 5201, ATC 5301 and ATC 540 containing the Systems Engineering content defined in this PMP for user comment review, ballot review, and approval.

2.2.1.7.1 Task 7.1 Develop User Comment Draft (UCD) ATC Standards

Objectives

- Develop the Working Group Draft (WGD) and UCD versions of ATC 5201, ATC 5301 and ATC 5401 with cybersecurity content.

Approach

- Update each ATC standard so that they conform to the ATC Cybersecurity Standard.
- The systems engineering content in the ATC Cybersecurity Standard may or may not be used directly in the ATC standards.
- The ATC standards will be updated according to their current levels or form of SEP content.
- Prepare and deliver a Working Group Draft (WGD) Standard.
- Prepare and deliver a proposed UCD (pUCD) for acceptance of the ATC Joint Committee as a UCD.
- Conduct/support the SDO user comment process and prepare a resolution sheet for the UCD

comments.

- The ATC WGs adjudicate the comments received and come to a consensus on the updates to the UCD that are to be performed.
- Distribute the adjudicated comments in a Comment Disposition Report.
-

Deliverables

- WGD ATC 5201 Standard [PWS Deliverable]
- WGD ATC 5301 Standard [PWS Deliverable]
- WGD ATC 5401 Standard [PWS Deliverable]
- UCD ATC 5201 Standard [PWS Deliverable]
- UCD ATC 5301 Standard [PWS Deliverable]
- UCD ATC 5401 Standard [PWS Deliverable]
- UCD ATC 5201 Standard Comments Disposition Report [PWS Deliverable]
- UCD ATC 5301 Standard Comments Disposition Report [PWS Deliverable]
- UCD ATC 5401 Standard Comments Disposition Report [PWS Deliverable]

2.2.1.7.2 Task 7.2 Develop Ballot and Final ATC Standards

Objectives

- Develop the Recommended Standard (RS) and Jointly Approved versions of ATC 5201, ATC 5301 and ATC 5401 with cybersecurity content.

Approach

- For each UCD ATC standard, revise the standard to address the UCD comments and resolutions.
- A proposed RS (pRS) ballot-ready will be prepared by the standard working group and submitted to the relevant Joint Committee for acceptance as an RS.
- ITE will support the comment resolution and updates of the RS until all ballot comments have been resolved to the satisfaction of the SDOs and USDOT.
- Once all of the SDOs involved have approved the standard, ITE will prepare a publication ready Jointly Approved Standard and publish.

Deliverables

- RS ATC 5201 [PWS Deliverable]
- RS ATC 5301 [PWS Deliverable]
- RS ATC 5401 [PWS Deliverable]
- Jointly Approved ATC 5201 [PWS Deliverable]
- Jointly Approved ATC 5301 [PWS Deliverable]
- Jointly Approved ATC 5401 [PWS Deliverable]

2.2.2 Project Acceptance Criteria

Overall project acceptance is based on acceptance of the deliverables. Table 1 identifies the acceptance criteria and the accepting entity for each type of deliverable identified in the Section 2.2.1 Project Scope Description.

Table 1 Deliverable Acceptance Criteria and Accepting Entity

Deliverable Type	Acceptance Criteria	Acceptance By
Monthly Progress Reports	• Adherence to Section 4.1. • Meets quality control criteria as described in Section 5.3.	COR

Project Management Plan	• Adherence to Section 2.2.1.1.2. • Meets quality control criteria as described in Section 5.3.	USDOT
Systems Engineering Management Plan	• Adherence to Section 2.2.1.1.2. • Meets quality control criteria as described in Section 5.3.	USDOT
Comment Disposition Reports	• Criteria to be established by the PMT. • Meets quality control criteria as described in Section 5.3.	ATC WGs, PMT, USDOT
All Deliverable Engineering Documents and Standards	• Meets the objectives of the applicable project task (see Sections 2.2.1 and subtasks). • Meets quality control criteria as described in Section 5.3.	Steering Committee, PMT, USDOT

2.2.3 Project Exclusions

No exclusions have been identified.

2.2.4 Project Constraints

The following constraints have been established for the ATC Cybersecurity Project:
a) The project schedule may not extend beyond March 21, 2024.
b) Capital expenditures must be preapproved by ITE.
c) Project travel must be preapproved by ITE.

2.2.5 Project Assumptions

The following assumptions are being made for the ATC Cybersecurity Project:
a) Additional web conferences will be used as needed to meet the project goals.
b) Time has been built into many of the tasks due to the ATC WG reviews and process.
c) Throughout the project, there may be various versions of the project schedule produced to take advantage of economies discovered or to account for anomalies unforeseen. As long as there is no change in scope, this PMP does not need to be modified.

2.3 Scope Verification

It is the responsibility of the PM to verify interim project deliverables against the original scopeas defined in the scope description (see Section 2.2.1). If there is a proposed change of scope (see Section2.4), ITS JPO must formally accept the change prior to its incorporation into the project.

2.4 Scope Control

The PMT and the Project Team will work together to control the scope of the project. The Project Team will leverage the project scope description (see Section 2.2.1) andthe project schedule (see Section 4.3) as a statement of work for each task. The Project Team will ensure that they perform only the work described in the project scope description and generate the deliverables identified. The PMT will oversee the subcontracted Subject Matter Experts ("Subconsultant Team") and the progression of the project to ensure that this scopecontrol process is followed.

A change in scope is defined by a change in the overall budget, a change that extends the overall schedule, or a change in the work to be performed. Any member of the PMT, the subconsultant team, the Steering Committee, ATC WGs, or the ITS JPO may propose a change in scope. The proposed change is assessed by the PMT and subconsultant team. If the PMT and Subconsultant Team determine that a change in scope is warranted, formal approval from ITS JPO is required.This PMP is to be updated in the case of an approved change in scope.

3 COMMUNICATIONS PLAN

3.1 Purpose of the Communications Plan

This Communications Management Plan sets the communications framework for the administration of the ATC Cybersecurity Project. It identifies the key stakeholders, their roles, and contact information.

3.2 Stakeholder Points of Contact

ITS JPO Contracting Officer's Representative (COR)
Steve Sill, ITS Architecture & Standards Program Manager
ITS Joint Program Office
United States Department of Transportation
1200 New Jersey Avenue, SE, HOIT
Washington, DC 20590
Phone: 202-366-1603
Email: steve.sill@dot.gov

ATC Program Manager (PGM)
Siva R. K. Narla, Senior Director, Transportation Technology
Institute of Transportation Engineers
1627 I ("Eye") Street, NW, Suite 550
Washington, DC 20006
Phone: 202-464-6219
Email: snarla@ite.org

ATC Cybersecurity Project Manager (PM)
Nicola Tavares, Technical Projects Specialist
Institute of Transportation Engineers
1627 I ("Eye") Street, NW, Suite 550
Washington, DC 20006
Phone: 202-464-6208
Email: ntavares@ite.org

Technical Lead
Ralph W. Boaz, President
Pillar Consulting, Inc.
4511 Jicarillo Avenue
San Diego, CA 92117
Phone: 858-352-6281
Email: rboaz@pillarinc.com

ATC Cybersecurity Steering Committee Co-Chairs

Co-Chair A TBD

Co-Chair B TBD

ATC Joint Committee Chair
Dave Miller, Principal Systems Engineer
Yunex Traffic
9225 Bee Cave Road
Austin, TX 78733

Phone: 512-589-5749
Email: dave.miller@yunextraffic.com

ATC Controller Working Group Co-Chairs

John Thai, Principal Traffic Engineer
City of Anaheim
201 South Anaheim
City Hall West, Suite 502
Anaheim, CA 92805
Phone: 714-765-5294
Email: jthai@anaheim.net

Jim Rose, Hardware Engineering Manager
Econolite
1250 N Tustin Avenue
Anaheim, CA 92807
Phone: (714) 630-3700
Email: jrose@econolite.com

ATC API Working Group Co-Chairs

George Chen, Traffic Engineer
Los Angeles Department of Transportation
ATSAC Operations Division
100 S. Main Street, 9th Floor
Los Angeles, CA 90012
Phone: 213-972-5058
Email: george.chen@lacity.org

Douglas Tarico, Software Engineer Manager
Q-Free
970 Thomas Place
Vista, CA 92084
Phone: 760 207-7696
Email: douglas.tarico@q-free.com

ATC Cabinet Working Group Co-Chairs

Ahmad Jawad, Signal Systems Engineer
Road Commission for Oakland County
Email: ajawad@rcoc.org

Robert Rausch, Vice President
TransCore
Email: robert.rausch@transcore.com

ATC Standards Development Organization Liaisons

Robert T. White, Program Manager, Operations
American Association of State Highway & Transportation Officials (AASHTO)
555 12th Street NW, Suite 1000
Washington, DC 20004
Phone: 202-624-5497

Email: rwhite@aashto.org

Siva R. K Narla, Senior Director, Transportation Technology
Institute of Transportation Engineers (ITE)
1627 I (“Eye”) Street, NW, Suite 550
Washington, DC 20006
Phone: 202-785-0060 x119
Email: snarla@ite.org

Brian Doherty, Program Manager, Transportation Systems
National Electrical Manufacturers Association (NEMA)
1300 North 17th Street, Suite 900
Rosslyn, VA 22209
Phone: 703-841-3226
Email: brian.doherty@nema.org

Keith Wilson, Program / Business Development Manager
SAE International
755 West Big Beaver Road, Suite 1600
Phone: 248-273-2470
Email: kwilson@sae.org

3.3 Project Team and Steering Committee Communications

Communications within the subconsultant team is on an ad hoc basis. Meetings of the Steering Committee and ATC WGs will typically use web conferencing. Throughout the project, the ATC WGs will provide technical guidance and document reviews. The PM will work to ensure that the Steering Committee and ATC WG meetings are conducted according to the project needs.

3.4 Communications with ITS JPO

Communications between the Project Team and ITS JPO will formally take place once monthly and as deliverables occur as described in Section 4. It is anticipated that ITS JPO will have one ormore technical staff participating in the Steering Committee and ATC WG meetings and web conferences where they will have extemporaneous and informal communication with the Project Team. Official communicationsbetween ITS JPO and the Project Team should be made through the Program Manager and the COR (see Section 3.2).

4 DELIVERABLES AND MILESTONES

4.1 Monthly Progress Reports

ITE will provide monthly progress reports as follows:

a) Monthly Status Reports – ITE will submit monthly progress reports no later than 30 days after the end of the month being reported on in the format specified by the COR. The progress report will describe work completed during the period, anticipated work, problems encountered and and/or anticipated as well as financial status including at least hours expended and other costs.

b) Project Schedule – ITE will submit, to the Government, an initial project schedule in Microsoft Project Document (MPP) format within sixty (60) days after the effective date of the contract and updates showing the percent complete of major deliverables every thirty (30) days thereafter. The schedule will include at a minimum, the major deliverables and milestones and adhere to the Microsoft Project template structure provided by the COR. Any changes to due dates after the initial project schedule baseline must be approved by the Government. ITE will support the identification of schedule dependencies related to the project and in accordance with the Government defined process.

c) Risk Register – ITE will document risks that might affect the project and the characteristics of the risk defined by the ITS JPO. The COR will provide a Microsoft Excel-based Risk Register template for ITE to populate and update as necessary. Each risk will have a unique number, probability of occurrence and impact of occurrence rating. The risk log will be updated monthly and submitted with monthly progress reports.

ITS JPO templates are available at http://www.its.dot.gov/project_mang/index.htm

The Technical Lead will provide a monthly summary of the subconsultant team progress reports to the PM and an updated project schedule per the requirements for the PM's monthly reporting.

4.2 Deliverable Summary

Documents and software deliverables are to be sent electronically to the COR. Table 2 identifies the deliverables based on the project tasks identified on the initial project schedule in Section 4.3. The delivery dates identified for the initial schedule only. They may change through the course of the project.

Table 2 Deliverables by Project and Task

Proj Task	Deliverable Item	Delivery Date
1.2.2	Draft PMP with SEMP and Project Schedule [PWS Deliverable]	04/04/22
1.2.5	PMP with SEMP and Project Schedule [PWS Deliverable]	05/03/22
1.3.2	Monthly Progress Reports [PWS Deliverable]	Monthly no later than 30 days after the end of the month
2.1.3	Stakeholder and Subject Matter Expert List [PWS Deliverable]	06/08/22
2.1.6	Draft Stakeholder Interview Questionnaire [PWS Deliverable]	05/16/22
2.1.8	Stakeholder Interview Questionnaire [PWS Deliverable]	06/14/22
2.1.11	Draft Stakeholder Interview Summary Report	06/30/22
2.1.14	Stakeholder Interview Summary Report [PWS Deliverable]	07/19/22
2.1.16	Draft White Paper Summarizing Sources and Research	07/14/22
2.1.19	White Paper Summarizing Sources and Research [PWS Deliverable]	08/11/22
2.2.4	Draft ConOps [PWS Deliverable]	See MS Project Schedule 11/21/22
2.3.2	Draft ConOps Walkthrough Plan [PWS Deliverable]	07/18/22
2.3.5	ConOps Walkthrough Plan [PWS Deliverable]	08/03/22
2.3.8	ConOps Walkthrough Workbook [PWS Deliverable]	See MS Project Schedule 11/21/22
2.3.11	ConOps Walkthrough Comment Resolution Report [PWS Deliverable]	See MS Project Schedule 11/21/22
2.4.6	ConOps for ATC Cybersecurity Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
3.1.2	Draft SRS [PWS Deliverable]	See MS Project Schedule 11/21/22
3.2.2	Draft SRS Walkthrough Plan [PWS Deliverable]	See MS Project Schedule 11/21/22

Proj Task	Deliverable Item	Delivery Date
3.2.5	SRS Walkthrough Plan [PWS Deliverable]	See MS Project Schedule 11/21/22
3.2.8	SRS Walkthrough Workbook [PWS Deliverable]	See MS Project Schedule 11/21/22
3.2.11	SRS Walkthrough Comment Resolution Report [PWS Deliverable]	See MS Project Schedule 11/21/22
3.3.6	SRS for ATC Cybersecurity Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
4.1.2	Draft SDD [PWS Deliverable]	See MS Project Schedule 11/21/22
4.2.2	Draft SDD Walkthrough Plan [PWS Deliverable]	See MS Project Schedule 11/21/22
4.2.5	SDD Walkthrough Plan [PWS Deliverable]	See MS Project Schedule 11/21/22
4.2.8	SDD Walkthrough Workbook [PWS Deliverable]	See MS Project Schedule 11/21/22
4.2.11	SDD Walkthrough Comment Resolution Report [PWS Deliverable]	See MS Project Schedule 11/21/22
4.3.6	SDD for ATC Cybersecurity Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
5.1.13	UCD ATC Cybersecurity Standard	See MS Project Schedule 11/21/22
5.1.13	SDR for UCD ATC Cybersecurity Standard	See MS Project Schedule 11/21/22
5.1.17	UCD Comments Disposition Report	See MS Project Schedule 11/21/22
5.2.14	RS ATC Cybersecurity Standard	See MS Project Schedule 11/21/22
5.2.14	SDR for RS ATC Cybersecurity Standard	See MS Project Schedule 11/21/22
5.2.14	NOI for RS ATC Cybersecurity Standard	See MS Project Schedule 11/21/22
5.3.8	Jointly Approved ATC Cybersecurity Standard	See MS Project Schedule 11/21/22
6.3	ATC Cybersecurity Standard Test Plan [PWS Deliverable]	See MS Project Schedule 11/21/22
6.6	ATC Cybersecurity Test Report [PWS Deliverable]	See MS Project Schedule 11/21/22
7.1.1.2	WGD ATC 5201 Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
7.1.1.2	WGD ATC 5301 Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
7.1.1.2	WGD ATC 5401 Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
7.1.3.6	UCD ATC 5201 Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
7.1.3.6	UCD ATC 5301 Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
7.1.3.6	UCD ATC 5401 Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
7.1.3.10	UCD ATC 5201 Comments Disposition Report [PWS Deliverable]	See MS Project Schedule 11/21/22
7.1.3.10	UCD ATC 5301 Comments Disposition Report [PWS Deliverable]	See MS Project Schedule 11/21/22
7.1.3.10	UCD ATC 5401 Comments Disposition Report [PWS Deliverable]	See MS Project Schedule 11/21/22

Proj Task	Deliverable Item	Delivery Date
7.2.2.7	RS ATC 5201 Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
7.2.2.7	RS ATC 5301 Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
7.2.2.7	RS ATC 5401 Standard [PWS Deliverable]	See MS Project Schedule 11/21/22
7.2.4.3	Jointly Approved ATC 5201 [PWS Deliverable]	See MS Project Schedule 11/21/22
7.2.4.3	Jointly Approved ATC 5301 [PWS Deliverable]	See MS Project Schedule 11/21/22
7.2.4.3	Jointly Approved ATC 5401 [PWS Deliverable]	See MS Project Schedule 11/21/22

4.3 Project Schedule

The Gantt Charts in Figures 1 through Figure 6 provide the initial schedule for the ATC Cybersecurity Project Deliverable are identified by a diamond shape (◆). Web conferences are identified by a diamond shapewithin a circle (◈). Possible face-to-face meetings are identified by solid circle (●). The schedule may change through the course of the project and will be updated separately from this document.

See MS Project Schedule 11/21/22

Figure 1 ATC Cybersecurity Project Schedule (1 of 5)

See MS Project Schedule 11/21/22

Figure 2 ATC Cybersecurity Project Schedule (2 of 5)

See MS Project Schedule 11/21/22

Figure 3 ATC Cybersecurity Project Schedule (3 of 5)

See MS Project Schedule 11/21/22

Figure 4 ATC Cybersecurity Project Schedule (4 of 5)

See MS Project Schedule 11/21/22

Figure 5 ATC Cybersecurity Project Schedule (5 of 5)

5 QUALITY MANAGEMENT PLAN

5.1 Purpose of the Quality Management Plan

This Quality Management Plan describes how quality will be managed throughout the life of the project. It includes processes and practices for ensuring quality planning, quality control and quality assurance.

5.2 Quality Planning

In order to be successful, this PMP has integrated a quality system into the project tasks, project schedule, project deliverables and Project Team. The project relies heavily on the Steering Committee and ATC WGs to perform the role of a quality review team. The Steering Committee and ATC WGs are made up of subject matter experts including those from public agencies, manufacturers, software providers, and consulting firms.The Steering Committee and ATC WGs include operational users which provide quality input from the infrastructure community. The Steering Committee will also include one or more technical staff from ITS JPO. This allows the ITS JPO to have quality input early in the development of project deliverables. It is the responsibility of the Steering Committee Co-Chairs and the PMT to ensure that the Steering Committee is made up of individuals appropriate for the quality aspects of the project. The PMT and subconsultant team have been selected for their experience with the cybersecurity and the ATC standards.

There are two types of “quality” addressed by this plan: “product quality” and “process quality.” Product quality focuses on the project deliverables. Product quality will be insured by the Steering Committee and ATC WGs as described in the previous paragraph. Process quality focuses on how the project deliverables will be produced. The project scope description establishes multiple cycles of Steering Committee and/or ATC WG review, comment and comment resolution periods all directed at the aspect of quality.

5.3 Quality Control

This section describes the process for monitoring and recording the results of executing the quality activities. It applies to the project’s products as opposed to its processes.

The Steering Committee and/or ATC WG review of all project deliverables will be performed according to the project schedule. Additional reviews may be required to meet project objectives. Reviewers will verify that deliverable documents:

a) contain suitable material for the target audience;
b) are organized in presentation;
c) contain proper word use and English diction;
d) contain detailed illustrations;
e) are comprehensive, complete and technically correct; and
f) are edited for grammatical and editorial errors.

Project deliverables will be judged on a “suitable for purpose” basis. The Project Team may identify more items or make suggestions for changes to a document than are needed to meet the project goals. In some cases, gaining consensus on technical matters within a committee can be time consuming.If any undertaking by a committee may jeopardize the project schedule, the PMT may make decisions and recommendations to move the project forward.

5.4 Quality Assurance

A Quality Checklist will be established and maintained by the PMT to assist in identifying specific items to be reviewed by the ATC WGs. A Project Issue Log will be established and maintained by the PMT to capture any issue regarding the project that should be addressed by the Project Team including items that pertain to quality. Items for the Quality Checklist and Project Issue Log may be proposed by any member of the Project Team. It is up to the PMT to determine if these items should be included on these lists and if any action should be taken. The PMT will discuss any quality items on a bi-weekly basis.

6 HUMAN RESOURCES MANAGEMENT PLAN

6.1 Purpose of the Human Resources Management Plan

This Human Resources Management Plan is a tool which aides in the management of the human resources throughout the ATC Cybersecurity Project. It contains the roles, responsibilities and reporting on the project.

6.2 Roles, Responsibilities and Reporting

Table 3 identifies the members of the Project Team, their roles within the project, their project responsibilities, and their reporting responsibilities.

Table 3 Project Team and Reporting

Name	Project Role	Responsibilities	Reporting
Ralph W. Boaz Pillar Consulting 714-803-0330 rboaz@pillarinc.com	Technical Lead, SE, SME	• Part of the Project Management Team. • Part of the Subconsultant Team. • Assists ITE to maintain project reporting required by the USDOT. • Quality management function on deliverables. • Provides leadership for the rest of the consulting team. • Coordinates with the Chairs of the Steering Committee, Controller WG, API WG and Cabinet WG. • Creation and maintenance of PMP and SEMP preparation. • Provides expertise in CV technology, ATC equipment, NTCIP communications, and testing.	• Weekly progress reports with Project Team. • Provides monthly project status reports to the PM per Section 4.1.
Patrick Chan ConSysTec 917-497-6718 patrick.chan@consystec.com	SE, SME	• Part of the Subconsultant Team. • Provide feedback on technical deliverables as appropriate. Forexample, ConOps, SRS, and SDD documents. • Participates in technical reviews (e.g., walkthroughs) of the technical deliverables. • Provides Q/A function. • Provides expertise in CV technology, NTCIP communications, and testing.	• Weekly progress reports with Project Team.
Ajay Chandra Chintamaneni Gurus Infotech ajay@gurusinfotech.net	SE	• Part of the Subconsultant Team. • Provide feedback on technical deliverables as appropriate. Forexample, ConOps, SRS, and SDD documents. • Participates in technical reviews (e.g., walkthroughs) of the technical deliverables.	• Weekly progress reports with Project Team.
A. Jay Lahiri ConSysTec 646-874-9289 ajl@consystec.com	SE	• Part of the Subconsultant Team. • Provide feedback on technical deliverables as appropriate. Forexample, ConOps, SRS, and SDD documents. • Participates in technical reviews (e.g., walkthroughs) of the technical deliverables.	• Weekly progress reports with Project Team.
Uma Mahesh Madineni Gurus Infotech 703-870-0890 mahesh@gurusinfotech.net	PM Support	• Part of the Subconsultant Team. • Supports PGM, PM and Technical Lead. • Meetings, records, collaboration tools.	• Weekly progress reports with Project Team.

Name	Project Role	Responsibilities	Reporting
Narla, Siva ITE (202) 464-6219 snarla@ite.org	ATC Program Manager	• Part of the Project Management Team. • Official administration and coordination of the project from a contracts perspective. • Monitors project expenditures in labor, travel expenses and capital expenses. • Official project communications channel to the COR. • Coordinates and supports the Steering Committee. • Co-Creation of PMP.	• Provides monthly progress reports to the COR per Section 4.1 including an updated Microsoft Project Schedule.
Purna Nimmagadda Gurus Infotech 703-868-3426 purna@gurusinfotech.com	Requirements Analyst	• Part of the Subconsultant Team. • Provide feedback on technical deliverables as appropriate. Forexample, ConOps, SysReq and SDD documents. • Participates in technical reviews (e.g., walkthroughs) of the technical deliverables.	• Weekly progress reports with Project Team.
Tiffany Rad ELCnetworks (202) 507-9441 tiffany@anatrope.com	SME	• Part of the Subconsultant Team. • Provide feedback on technical deliverables as appropriate. Forexample, ConOps, SysReq and SDD documents. • Participates in technical reviews (e.g., walkthroughs) of the technical deliverables.	• Weekly progress reports with Project Team.
Deborah Rouse ITE 202-785-0060 drouse@ite.org	Technical Editor	• Ensures project documents contain suitable material for the target audience. • Ensures project documents are organized in presentation. • Reviews project documents for grammatical and editorial errors. • Reviews project documents for proper word use and English diction.	• Provides weekly reports when tasked with a specific deliverable.
Tatiana Richey ITE (202) 785-0060 ntavares@ite.org	Contracts Manager	• Official administration and coordination of the project from a contracts perspective. • Prepares project policies and procedures to fulfil contract requirements.	• Provides weekly reports to the PGM and PM.
Tavares, Nicola ITE (202) 464-6208 ntavares@ite.org	Project Manager	• Part of the Project Management Team. • Official administration and coordination of the project from a contracts perspective. • Monitors project expenditures in labor, travel expenses and capital expenses. • Official project communications channel to the COR. • Supports the Steering Committee . • Maintains communication and consensus building within the WG. • Organizes meetings and keeps records.	• Provides monthly progressreports to the COR per Section 4.1 including an updated Microsoft Project Schedule.

Name	Project Role	Responsibilities	Reporting
Michaela Vanderveen Independent Consultant	SME	• Part of the Subconsultant Team. • Provide feedback on technical deliverables as appropriate. Forexample, ConOps, SysReq and SDD documents. • Participates in technical reviews (e.g., walkthroughs) of the technical deliverables.	• Weekly progress reports with Project Team.
TBD	Steering Committee Co-Chair	• Part of the Project Management Team. • Provides leadership of the Steering Committee. • Presides over Steering Committee meetings. • Focuses the effort of the Steering Committee to provide feedback to subconsultant team in a timely fashion. • Builds consensus with the Steering Committee members.	• Weekly progress reports with Project Team.
TBD	Steering Committee Co-Chair	• Part of the Project Management Team. • Provides leadership of the Steering Committee. • Presides over Steering Committee meetings. • Focuses the effort of the Steering Committee to provide feedback to subconsultant team in a timely fashion. • Builds consensus with the Steering Committee members.	• Weekly progress reports with Project Team.

6.3 Organizational Chart

Figure 1 shows an organizational chart for ATC Cybersecurity Project. The chart shows the project team including the ATC working groups due to their critical role in providing expertise subject matter expertise and their rolls in the developing the ATC standards towards the end of the project. The organization is somewhat flat with some members of the Steering Committee and WGs serving in multiple groups. It is expected that there will be significant collaboration between the Technical Lead and the co-chairs and the various groups. Supporting roles are shown but they are not considered a part of the project team.

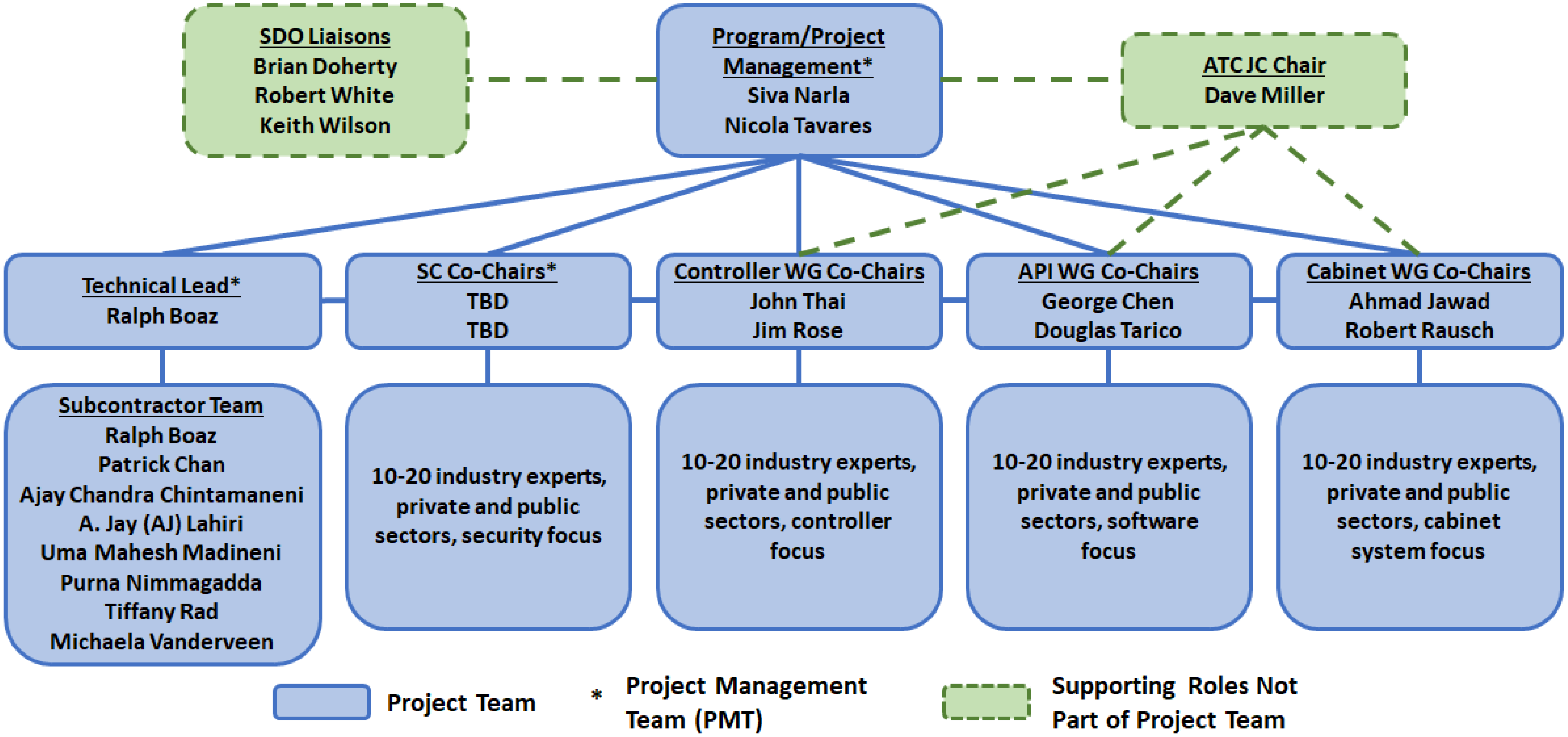

Figure 6 ATC Cybersecurity Project Organization

7 SYSTEMS ENGINEERING MANAGEMENT PLAN

7.1 Purpose of the Systems Engineering Management Plan

This Systems Engineering Management Plan (SEMP) establishes a common understanding of how the systems engineering portions of the project will be organized, structured, conducted and controlled to meet the project goals for:

a) The USDOT Intelligent Transportation Systems (ITS) Joint Program Office (JPO) who is sponsoring the work.

b) The partner Standard Development Organizations (SDOs) who are representing stakeholders for this project.

c) The project team contracted to perform the work.

d) The ATC Cybersecurity Steering Committee as the oversight group to develop standards relevant to cybersecurity of ATC standards under this task.

e) The broad stakeholder community made up infrastructure, cybersecurity, and connected vehicle communities represented by AASHTO, NEMA, SAE, ITE and others.

The organization of this SEMP is derived from the Systems Engineering Plan described in the International Council on Systems Engineering (INCOSE) Systems Engineering Handbook, Version 3.2 and IEEE Std 1220-2005, IEEE Standard for Application and Management of the Systems Engineering Process.

7.2 Systems Engineering Process Application

7.2.1 Systems Engineering Process Planning

The central activity of the ATC Cybersecurity Project is the development of standard to allow the transportation infrastructure community to deploy field equipment that is secure and a foundation for other ITS and possibly non-ITS applications. A systems engineering process (SEP) is being applied to the ATC Cybersecurity Project incorporating layers of review and modification of the deliverable documents to minimize development risk. Sections 2.2.1 and 4.3 provide the details of the tasks and schedule. The primary objectives of this project are to: a) establish and maintain a cohesive project management plan; b) deliver an approved ATC Cybersecurity Standard; and c) to provide stakeholder input based on actual product development.

7.2.2 Process Inputs

Inputs to this systems engineering process are as follows:

- ATC standards ATC 5201 v06A, ATC 5401 v02A, and ATC 5301 v02
- NCHRP 03-127 Cybersecurity of Traffic Management Systems
- CIS Controls Version 7 Implementation Guidance for Industrial Control Systems
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- NIST Special Publication 800-53
- NIST Special Publication 800-82r2
- NIST Framework for Improving Critical Infrastructure Cybersecurity

7.2.3 Technical Objectives

The technical objectives for the ATC Cybersecurity Project are identified in the project scope description found in Section 2.2.1 of this document.

7.2.4 Training

The subconsultant team will receive training on the ATC standards and ITS systems as part of the work through team meetings. Most members of the team are at a senior level technically and most have had projects in ITS. They bring their expertise from various fields to develop cybersecurity for the ATC standards and deploying secure ITS field equipment.

7.2.5 Standards and Procedures

Table 4 identifies the standards or procedures used in the production of the project deliverables. (Note: this table uses the Task numbers identified in Section 2.2). If there are multiple drafts of a deliverable item, only the first version of the deliverable is listed. All the other versions of the deliverable will use the same standard or procedure.

Table 4 Deliverable Items and Associated Standards or Procedures

Proj Task	Deliverable Item	Standard or Procedure
1.2.5	PMP with SEMP and Project Schedule [PWS Deliverable]	As described in Section 2.2.1.1.2 of this document.
1.3.2	Monthly Progress Reports [PWS Deliverable]	As described in Section 4.1.
2.1.19	White Paper Summarizing Sources and Research [PWS Deliverable]	None
2.1.3	List of Stakeholders and Subject Matter Experts [PWS Deliverable]	None
2.1.8	Stakeholder Interview Questionnaire [PWS Deliverable]	None
2.1.14	Stakeholder Interview and Questionnaire Report Summary [PWS Deliverable]	None
2.1.19	White Paper Summarizing Sources and Research [PWS Deliverable]	None
2.2.4	Draft ConOps [PWS Deliverable]	ISO/IEC/IEEE 29148:2011, NTCIP 8002 Annex B1, PWS, Appendix B, Section 2
2.3.2	Draft ConOps Walkthrough Plan [PWS Deliverable]	IEEE Std 1028-2008
2.3.8	Walkthrough Workbook for ConOps Review	IEEE Std 1028-2008
2.3.11	ConOps Walkthrough Comment Resolution Report [PWS Deliverable]	None
3.1.2	Draft SRS [PWS Deliverable]	ISO/IEC/IEEE 29148:2011, PWS, Appendix B, Section 3
3.2.2	Draft SRS Walkthrough Plan [PWS Deliverable]	IEEE Std 1028-2008
3.2.8	Walkthrough Workbook for SRS Review	IEEE Std 1028-2008
3.2.11	SRS Walkthrough Comment Resolution Report [PWS Deliverable]	None
4.1.2	Draft SDD [PWS Deliverable]	IEEE Std 1016-2009, PWS, Appendix B, NTCIP 8002 Annex B1
4.2.2	Draft SDD Walkthrough Plan [PWS Deliverable]	IEEE Std 1028-2008
4.2.8	Walkthrough Workbook for SDD Review	IEEE Std 1028-2008

Proj Task	Deliverable Item	Standard or Procedure
4.2.11	SDD Walkthrough Comment Resolution Report [PWS Deliverable]	None
5.1.13	UCD ATC Cybersecurity Standard	NTCIP 8002 Annex B1
5.1.13	SDR for UCD ATC Cybersecurity Standard	Per ITE Practice
5.1.17	UCD Comments Disposition Report	None
5.2.14	SDR for RS ATC Cybersecurity Standard	Per ITE Practice
5.2.14	NOI for RS ATC Cybersecurity Standard	Per ITE Practice

7.2.6 Systems Engineer Role

The Systems Engineer (SE) role has a broader influence in the ATC Cybersecurity Project than that of traditional SE roles. Responsibilities include:

- Support task forces in research and interview process and identifying user needs.
- Collecting user needs from task forces.
- Preparing and maintaining the SEMP.
- Developing the ConOps and SRS documents.
- Assisting with systems engineering portions of design documents.
- Leading walkthroughs of documents at various stages of the project.
- Providing the overall project rigor required to verify that complete and correct project products are being developed.
- Ensuring traceability throughout project documents as appropriate.

General resource levels for the Systems Engineer are shown in Table 5. Resource levels are categorized as follows:

a) Primary – The task is primarily an SE function.
b) Secondary – The SE plays a secondary role in the task.
c) Advisory – The SE plays a small or advisory role in the task.
d) N/A – The task does not apply to the SE.

Table 5 Resource Levels for the Systems Engineer

Proj Task	Project Task	Resource Level
1.1	Kick-Off Meeting	Advisory
1.2	Project Management Plan and Systems Engineering Management Plan	Primary
2.1	Review Relevant Prior and Ongoing Research	Primary
2.2	Develop Draft Concept of Operations	Primary
2.3	Walkthrough on Draft Concept of Operations	Primary
2.4	Final Concept of Operations	Primary
3.1	Develop Draft System Requirements Specification (SRS)	Primary
3.2	Walkthrough on Draft SRS	Primary
3.3	Final System Requirements Specification	Primary
4.1	Develop Draft System Design Description (SDD)	Primary
4.2	Walkthrough on Draft SDD	Primary
4.3	Final System Design Description	Primary
5.1	Develop User Comment Draft ATC Cybersecurity Standard	Primary
5.2	Develop Recommended Standard ATC Cybersecurity Standard	Primary
5.3	Develop Approved ATC Cybersecurity Standard	Primary
6	Develop and Perform ATC Cybersecurity Standard Verification and Validation	Primary

Proj Task	Project Task	Resource Level
7.1	Develop User Comment Draft (UCD) ATC Standards	Primary
7.2	Develop Ballot and Final ATC Standards	Primary

7.2.7 Work Authorization

Specific work authorization is required at the following points in the ATC Cybersecurity Project:

- Task 1.4 Authorization to Proceed is required from USDOT before advancing to Task 2 Develop Concepts of Operations (ConOps) for the ATC Cybersecurity Standard.
- Task 6.1 Receive Authorization to Proceed is required from USDOT before the remainder of the work on Task 6 Develop and Perform ATC Cybersecurity Standard Verification and Validation.

7.3 Systems Analysis and Control

This section describes how the systems engineering portions of the project will be performed and controlled. Included are the project team organization, a configuration management plan, a verification and validation plan and a risk management plan.

7.3.1 Configuration Management Plan

It is intended that each deliverable document and will be maintained under an electronic configuration management system which includes issue tracking.

7.3.1.1 Configuration Management of the ATC Cybersecurity Project

The products delivered under this project will use version numbering to uniquely identify draft documents that are circulated for review, comment, acceptance and approval within the project team, the Steering Committee, the ATC standards WGs, and the SDOs. The systems engineering documents ConOps,SRS, SDD, and the software developed under this SEMP will use versioning in the form "XX.YY" where: "XX" is the twodigit major revision number, and "YY" is the two digit minor revision number. Whenever a document or software is to be circulated, the author will increment the minor revision number or letter whichever is appropriate prior to circulation. The author may increment the version of a document multiple times for his or her own configuration management purposes. If a document is being edited by multiple people simultaneously, one person will be designated by the project manager as editor-in-chief (EIC). In this case, the EIC will gather the document changes, paragraphs, sections, etc. from the other authors and be responsible for sending out the draft document with a new version number. All documents developed under this SEMP will start with a major revision number of 01.

The Project Manager, the Technical Lead, and the various WG chairs will function as a configuration management board. They will determine when project products are suitable for coming under configuration management. Table 6 lists the project products which are the baseline items to come under configuration management.

Table 6 Project Products for Baseline Configuration Management

Proj Task	Configuration Management Baseline Item
1.2.2	Draft PMP with SEMP and Project Schedule [PWS Deliverable]
1.2.5	PMP with SEMP and Project Schedule [PWS Deliverable]
2.1.3	Stakeholder and Subject Matter Expert List [PWS Deliverable]
2.1.6	Draft Stakeholder Interview Questionnaire [PWS Deliverable]

Proj Task	Configuration Management Baseline Item
2.1.8	Stakeholder Interview Questionnaire [PWS Deliverable]
2.1.11	Draft Stakeholder Interview Summary Report
2.1.14	Stakeholder Interview Summary Report [PWS Deliverable]
2.1.16	Draft White Paper Summarizing Sources and Research
2.1.19	White Paper Summarizing Sources and Research [PWS Deliverable]
2.2.4	Draft ConOps [PWS Deliverable]
2.3.2	Draft ConOps Walkthrough Plan [PWS Deliverable]
2.3.5	ConOps Walkthrough Plan [PWS Deliverable]
2.3.8	ConOps Walkthrough Workbook [PWS Deliverable]
2.3.11	ConOps Walkthrough Comment Resolution Report [PWS Deliverable]
2.4.6	ConOps for ATC Cybersecurity Standard [PWS Deliverable]
3.1.2	Draft SRS [PWS Deliverable]
3.2.2	Draft SRS Walkthrough Plan [PWS Deliverable]
3.2.5	SRS Walkthrough Plan [PWS Deliverable]
3.2.8	SRS Walkthrough Workbook [PWS Deliverable]
3.2.11	SRS Walkthrough Comment Resolution Report [PWS Deliverable]
3.3.6	SRS for ATC Cybersecurity Standard [PWS Deliverable]
4.1.2	Draft SDD [PWS Deliverable]
4.2.2	Draft SDD Walkthrough Plan [PWS Deliverable]
4.2.5	SDD Walkthrough Plan [PWS Deliverable]
4.2.8	SDD Walkthrough Workbook [PWS Deliverable]
4.2.11	SDD Walkthrough Comment Resolution Report [PWS Deliverable]
4.3.6	SDD for ATC Cybersecurity Standard [PWS Deliverable]
5.1.13	UCD ATC Cybersecurity Standard
5.1.17	UCD Comments Disposition Report
5.2.14	RS ATC Cybersecurity Standard
5.3.8	Jointly Approved ATC Cybersecurity Standard
6.3	ATC Cybersecurity Standard Test Plan [PWS Deliverable]
6.6	ATC Cybersecurity Test Report [PWS Deliverable]
7.1.1.2	WGD ATC 5201 Standard [PWS Deliverable]
7.1.1.2	WGD ATC 5301 Standard [PWS Deliverable]
7.1.1.2	WGD ATC 5401 Standard [PWS Deliverable]
7.1.3.6	UCD ATC 5201 Standard [PWS Deliverable]
7.1.3.6	UCD ATC 5301 Standard [PWS Deliverable]
7.1.3.6	UCD ATC 5401 Standard [PWS Deliverable]
7.1.3.10	UCD ATC 5201 Comments Disposition Report [PWS Deliverable]
7.1.3.10	UCD ATC 5301 Comments Disposition Report [PWS Deliverable]
7.1.3.10	UCD ATC 5401 Comments Disposition Report [PWS Deliverable]
7.2.2.7	RS ATC 5201 Standard [PWS Deliverable]
7.2.2.7	RS ATC 5301 Standard [PWS Deliverable]
7.2.2.7	RS ATC 5401 Standard [PWS Deliverable]
7.2.4.3	Jointly Approved ATC 5201 [PWS Deliverable]
7.2.4.3	Jointly Approved ATC 5301 [PWS Deliverable]
7.2.4.3	Jointly Approved ATC 5401 [PWS Deliverable]

7.3.1.2 Comment Database Configuration Management

A comment database will be maintained throughout the entire project. The purpose will be to: a) capture comments both external and internal to the Steering Committee that are to be addressed and b) to maintain comments that are to be deferred for a future time if they are not addressed during this development. Duringthe development process, the formal comments will be reviewed by the Steering Committee, adjudicated as to theirrelevancy, and changes made to the documentation as appropriate. This comment database is separate from the Project Issue Log discussed in Section 5.4.

7.3.2 Verification and Validation Plan

Verification and validation (V&V) of whether the information content of the ATC Cybersecurity Standard document is complete and correct will rely on reviews of the pertinent information, summarized in the list below, and detailed in the subsequent technical review subsections:

a) The subconsultant team and the Steering Committee will perform at least two technical reviews of the ConOps, requirements content and design content.
b) The subconsultant team will perform a check for completeness and correctness of the user needs and requirements wording. The user needs and requirements are documented in the ConOps and the Requirements Specifications. The wording of each user need will be evaluated as expressing a major capability, being solution free, and capturing intent and rationale. The wording of each requirement statement will be checked for identifying a necessary attribute, capability, characteristic, or quality of the system in order for the system to have value and utility. This wording check will be presented to the Steering Committee and other stakeholders as part of respective Walkthroughs.
c) The subconsultant team and the Steering Committee will perform a check for logical completeness by performing a requirements traceability and consistency check. Requirement's traceability is documented in the NRTM and the RTM. This requirements traceability check will be presented to Steering Committee and other stakeholders as part of the SRS Walkthrough efforts.
d) The subconsultant team and the Steering Committee will perform a Design Content Consistency Check ofthe new Requirements content to the prior and/or revised system design details. This check will bepresented to the Steering Committee and other stakeholders as part of the SDD Walkthrough.
e) The UCD version, distributed to all interested parties with an invitation to submit proposed revisions (also known as "user comments"), is a customer-based V&V activity.
f) The pRS version, distributed to the Committee for review, comment and acceptance, is a V&V activity.

7.3.3 Walkthrough Reviews

Walkthroughs, sometimes referred to as "technical reviews," or "technical walkthroughs," provide a structured and organized approach to reviewing project products to determine if they are complete, correct, and accurate. Walkthroughs are used to identify defects (in needs, requirements or design) and identify alternative solutions at specified points in development (such as ConOps, SRS, and SDD). Walkthroughs are also used to clarify outputs (needs, requirements, or data concepts) and create a common understanding among the reviewers of the material. Walkthroughs represent the "control gates" that must be passed before the project can proceed to the next step in the development process.

Walkthroughs generally focus on technical "correctness" and logical consistency; however, in conjunction with the SRS Walkthrough, requirements traceability between needs and requirements (as reflected in NRTM) is evaluated; and, in conjunction with the SDD walkthrough, requirements traceability between requirements and design (as reflected in the RTM) is evaluated. The Steering Committee may schedule additional, subsequent reviews with the Project Team to provide support by web conference.

At least two weeks prior to each scheduled Walkthrough, the subconsultant team will develop a draft review output to be used in the conduct of the Walkthrough. This output is likely to include a draft Walkthrough workbook to guide Walkthrough participants in their review for logical consistency, quality of user needs and/or requirements, and (for SRS and SDD Walkthroughs) requirements traceability. The subconsultant team (assisted by the Steering Committee and stakeholders) will perform a logical consistency check, including a requirements traceability at appropriate points prior to or following Walkthroughs.

The Walkthrough workbook will be used to manage revisions identified during the walkthrough. Officially submitted or external comments received prior to or following the Walkthroughs will be entered into the proposed revision database. Editorial proposed revisions, such as grammar and spelling, do not have to be disposed of during the Walkthrough or entered in the proposed revision database and can be addressed directly by the subconsultant team. However, as a part of each Walkthrough, any entry in the proposed revision database that may impact the Walkthrough will be brought to the attention of Walkthrough participants for consideration. Any changes to the proposed revision database (new comments and resolutions to old comments) resulting from the Walkthrough will be entered in the proposed revision database, for subsequent consideration. Informal comments, such as those that may arise during a Walkthrough, may not be entered in the proposed revision database; rather, the draft resulting from the Walkthrough serves to capture proposed revisions.

Beyond addressing the comments received, the format of and procedures used for each Walkthrough and subsequent review will vary by subtask and depending on whether the review is of the first draft of ConOps or later walkthroughs. For example, the ConOps Walkthrough may only consist of a page by page review of the user needs for correctness and logical consistency; while the SRS Walkthrough should consist of a review for correctness and logical consistency, as well as requirements traceability. The SDD Walkthrough will review content from the design document as part of its logical consistency and traceability check, which may result in revision of the ConOps. Or, at later stages, only content that has changed since the ConOps Walkthrough may be subjected to logical consistency and requirements traceability checks. Regardless, IEEE 1028-2008 Section 7 will be used as a reference to design and conduct the Walkthrough, and the format and procedures to be used for that walkthrough will be included in the draft review output prior to the Walkthrough.

7.3.4 Requirements Traceability and Logic Check

One of the key controls and validation activities of the development is tracing requirements. This tracing will occur in two directions - backward to the user needs defined in the ConOps, and forward to the specification of design details.

Two types of traceability will be managed throughout the development process:

a) User needs to requirements traceability, called needs-to-requirements traceability; and
b) Requirements to design traceability, called requirements traceability.

7.3.4.1 User Needs to Requirements Traceability and Logic Check

The Steering Committee and stakeholders will review and comment on the check of needs and requirements performed by the subconsultant team to ensure that all user needs are defined and that the requirements stated satisfy a particular user need. The user needs to requirements traceability is documented in the NRTM. The NRTM forms the basis for this check and it is reviewed by the stakeholders.

The subconsultant team anticipates holding at least one Walkthrough in Washington, D.C. to enable the participation of all SDO staff and the ITS JPO support staff.

The NRTM lists all the user needs in the ConOps and is used to verify that all the user needs have been satisfied by at least one requirement. The NRTM will be created after the completion of the ConOps, and then will be updated at each remaining step of the development process. The logical association of the user needs and their associated requirements will be evaluated. Illogical associations will be eliminated, or statement wording will be revised.

The goals and technical approach of the logical consistency check is to ensure that the organizational list of the concepts (the user needs and requirements) make a logical framework that makes sense to the stakeholders. Requirements traceability and logical consistency checks are the responsibility of the subconsultant team, the Steering Committee, and the stakeholders, as part of the ConOps and SRS Walkthroughs. The concepts should flow from broad to narrow, or in some other easily recognized framework. The technical approach can include listing in a table (e.g., the NRTM), organizing, diagramming, charting, or using other graphical techniques to build and visualize a framework. Walkthrough workbooks are anticipated for both the ConOps and SRS Walkthroughs to guide review of technical correctness and traceability.

7.3.4.2 Requirements to Design Traceability and Logic Check

During the SDD Walkthrough, the subconsultant team, the Steering Committee, and stakeholders will review and comment on the mapping of requirements to design elements to ensure that all requirements are satisfiedby the design elements. The Requirements to Design traceability will be documented in the RTM. The RTM forms the basis for this check and its review by stakeholders. In this way, the RTM will be used to verify and validate that a dialog satisfies one or more information exchange requirements. A Walkthroughworkbook is also anticipated prior to the SDD Walkthrough to guide review.

The RTM will map from requirements to design details. Each requirement will map to one and only design detail. The RTM will be created after the completion of the requirements content, then will be updated at each remaining step of the development process.

Logical consistency checks remain the responsibility of the subconsultant team, the Steering Committee, and stakeholders, as part of the SDD Walkthrough. The subconsultant team will provide periodic reminders to the Steering Committee and stakeholders, so that this responsibility is not overlooked.

Upon completion of the RTM, the subconsultant team will perform a traceability check of ATC Cybersecurity Standard for any orphan design details that may have been overlooked as part of the preceding Walkthroughs, e.g., any dialogs, data objects, or block objects that have not been mapped to a requirement. Those orphan design details will be reviewed with the Steering Committee to determine if any user need and requirement can be identified that the design details can be mapped to. If no user need and requirement can be identified for an orphan design detail, that design detail will be deprecated for the ATC Cybersecurity Standard.

When the project reaches Task 5.1, each Systems Engineering (SE) element will have been considered during at least one walkthrough, and during at least one walkthrough, participants will have considered a “logical consistency check” signified by a question for each SE element in a walkthrough workbook. For each SE element, participants are asked a question of the form: “Is the [systems engineering element] logically consistent with [the related systems engineering element(s)]?” The logical consistency check is, by its nature:

a) Subjective - requiring a moment of critical thinking by each walkthrough participant, regardingeach Systems Engineering element (user need, requirement, SDD, or test case); and
b) Incremental - conducted as part of each walkthrough.

To restate, it is anticipated that, logical consistency for each SE element is evaluated:

a) when new SE elements are developed, or when existing SE elements are revised by the Systems Engineer.
b) during at least one walkthrough, as SE elements are developed and traced (when walkthrough participants consider the question “is this SE element logically consistent?”); and finally,
c) at this stage, logical consistency is evaluated for SE elements, to ensure that SE elements are “clear, concise and properly constructed ensuring proper communication is translated into the document and reflected in the design” is verified.

7.3.5 Risk Management Plan

This section identifies potential problems in the project before they occur, plans for their occurrence, and monitors the system development so that early actions can be taken. A Risk Log has been established as shown in Table 7. Using this log risks can be identified, analyzed, prioritized, and mitigated.

Risk monitoring will be performed by the project manager on a bi-weekly basis. Each risk area addressed in this PMP will be reviewed along with any new risk area that is identified during the execution of the project. At any time during the project any member of the Steering Committee or interested parties may alert the management team of the occurrence of a risk item or identify new risk areas. New risk areas identified willbe added to a Risk Log Table maintained by the project manager in a format specified by the USDOT.

Table 7 Risk Log

ID#	ProjectWork Stream	Status	Risk Category	Description	Impacts	Owner	Risk Response Plan (update where applicable)	Date Assessed	(P)	(I)	P*I	Priority
1	ATC Cybersecurity Standard	Identified	Technical	Insufficient participation from different stakeholder groups	High	PMT	See below.	02/25/22	1	3	3	4
2	ATC Cybersecurity Standard	Identified	Technical	Incorrect or incomplete inputs on user needs and/or requirements	Medium	PMT	See below.	02/25/22	2	2	4	2
3	ATC Cybersecurity Standard	Identified	Technical Schedule Cost	User needs or requirements are discovered late in the process	Medium	PMT	See below.	02/25/22	1	2	2	5
4	ATC Cybersecurity Standard	Identified	Schedule	Typical WG review and consensus building is difficult for development teams.	Medium	PMT, SC/WG Chairs	See below.	02/25/22	2	2	4	2
5	ATC Cybersecurity Standard	Identified	Schedule	Insufficient time to compete ATC Cybersecurity Standard	High	PMT	See below..	02/25/22	2	3	6	1

LEGEND:
ID# – Unique identifier for each identified risk item.
Project Work Stream – Specific contract/task order activity and/or deliverable to which the risk item applies.
Status – Current status of the risk item (Identified/In Progress/Retired)
Risk Category –

a) Schedule – Risks that cause schedule slippage of the project;
b) Cost – Risks that cause cost to exceed budget of the project; and
c) Technical – Risks affecting the completeness or correctness of the product.

Impacts – Impacts on the task or program if the identified risk occurs.
Owner – Individual or entity with authority to resolve risk.
Risk Response Plan – Description of the planned response should an identified risk occur. This column can be a reference to a specific plan document.
Date Assessed – Most recent date the risk and/or risk response plan was updated.
(P) – See Table 5 below.
(I) – See Table 5 below.
P*I – Risk probability (P) multiplied by impact of risk (I).
Priority - Identifies priority based on the P*I. The lower the number, the higher the priority.

Table 8 Values Assigned for Probability of Risk and Impact of Risk

Probability of Occurrence (P)	Impact of Risk (I)
3 = High Certain or highly likely to occur	**3 = High** Major impact on cost, schedule, or scope
2 = Medium 50/50 chance of occurring	**2 = Medium** Significant impact on cost, schedule or scope
1 = Low Possible, but unlikely to occur	**1 = Low** Insignificant impact on cost, schedule, or scope

Risk Item Details

Risk Item #1: Insufficient participation from different stakeholder groups

The risk is that the stakeholders participating will not be sufficient to provide the use-cases, needs and requirements to meet the goals of the project. This could occur at the beginning of the project as the project is gaining momentum and it could occur at various other points of the project when participants are needed with specific skillsets.

Mitigation:

The mitigations options identified are:

a) Utilize the broad base of stakeholders already identified in the PMP including SDO liaisons, working groups, resent past projects, the ITE Community groups for ATC standards and TSMO, the CAT Coalition, and other signal systems and cybersecurity communities. Examples include the Transportation Research Board (TRB) Signal Systems Committee (ACP25), Standing Committee on Systems, Enterprise, and Cyber Resilience (AMR40), Critical Infrastructure Standing Committee (AMR10), and Standing Committee on Regional Transportation Systems Management and Operations (ACP10).
b) Identify in advance, the stakeholder needs for the next period of development, key individuals (if possible) and their availability, and ensure the expertise needed is available for the project.

Risk Item #2: Incorrect or incomplete inputs on user needs and/or requirements

The risk is that the subconsultant team does not get correct or complete inputs on user needs and requirements through the stakeholder interviews and reviews.

Mitigation:

The mitigation options identified are:

a) Mitigation options in Risk Item #01.
b) Develop or update operational scenarios as part to cover missing areas.
c) Interim draft documents may be sent outside of the project team during development to get additional input.
d) Add additional expertise to the project team if necessary.

Risk Area #3: User needs or requirements are discovered late in the process

The risk is that new user needs or requirements are discovered beyond the time scheduled for their development. Some revisions of previous development phases are expected as the project advances. This could happen as new stakeholders become involved during the development process or when developing design elements uncover a new issues that are beyond what is expected.

Mitigation:

The mitigation options identified are:

a) The PMT may activate a Quick Response Group (QRG) that is representative of the Steering Committee to address any late userneeds or requirements that may be received.
b) The late user needs or requirements may be deferred to another version of the standard.

Risk Area #4: Typical committee review and consensus building is difficult for development teams

The risk is that gaining consensus on technical matters within a committee or WG can be time consuming and even stall jeopardizing the project schedule.

Mitigation:

The mitigation options identified are:

a) The PMT may activate a QRG to be representative of the Steering Committee.
b) Steering Committee Co-Chairs may make decisions for the group if consensus cannot be achieved.

Risk Area #5: Insufficient time to complete the ATC Cybersecurity Standard

The risk is that there is insufficient time to finish the development of a fully complete ATC Cybersecurity Standard. standard going throughall the steps of the standards development process of the participating SDOs within the period of performance. The development of a standard for an SDO involves well-defined steps that must be completed prior to balloting, approval, and publishing a standard by the SDO. Given the start time for this new standard, there is risk that it will not be completed.

Mitigation:
The mitigation options identified are:

a) Ensure that other tasks in the project beyond that of the developing the standard do not compete for resources with the tasks that are developing the standard.
b) Complete the development of the standard only to an earlier deliverable (e.g., Recommend Standard instead of a Jointly Approved Standard).
c) Consider the development of a guidance document instead of a standard. In this case, the document will still go through a systems engineering process, a user comment phase, and update; but the lengthy SDO approval process is not necessary. In this case, the changes to the ATC standards are implemented outside of this project.

APPENDIX A REFERENCES

USDOT ITS Joint Program Office, *Performance Work Statement for Institute of Transportation Engineers (ITE) Connected Signalized Intersection, Contract* 693JJ321D000005 *, Task Order* 693JJ321F000419 . USDOT ITS Joint Program Office, 2021.

ISO/IEC/IEEE, *ISO/IEC/IEEE 24748-4-2016, International Standard for Systems and Software Engineering -- Life Cycle Management -- Part 4: Systems Engineering Planning,* 2016

ISO/IEC/IEEE, *ISO/IEC/IEEE 15288:2015, Systems and software engineering -- System life cycle processes,* 2015

ISO/IEC/IEEE, *ISO/IEC/IEEE 29148:2011, Systems and software engineering -- Life cycle processes -- Requirements engineering*, 2011

IEEE, *IEEE Std 1016-2009 IEEE Standard for Information Technology--Systems Design--Software Design Descriptions,* 2009

IEEE, *IEEE Std 1028-2008, IEEE Standard for Software Reviews and Audits,* 2008

IEEE, *IEEE Std 1220-2005, IEEE Standard for Application and Management of the Systems Engineering Process,* 2005

Advanced Transportation Controller (ATC) Websites
https://www.ite.org/technical-resources/standards/atc-controller/
https://www.ite.org/technical-resources/standards/atc-api/
https://www.ite.org/technical-resources/standards/its-cabinet/

National Transportation Communications for ITS Protocol (NTCIP) Website:
https://www.ntcip.org

ITS Joint Program Office (JPO) Templates:
http://www.its.dot.gov/project_mang/index.htm

Other Websites:
https://attack.mitre.org/
https://collaborate.mitre.org/attackics/index.php/Main_Page

APPENDIX B GLOSSARY, ACRONYMS AND ABBREVIATIONS

Term	Definition
AASHTO	American Association of State Highway and Transportation Officials
ANSI	American National Standards Institute's
API	Application Programming Interface
ATP	Authorization to Proceed
AV	Automated Vehicles
CAT	Cooperative Automated Transportation
CO	Contracting Officer
ConOps	Concept of Operations
COR	Contract Officer's Representative
CI	Connected Intersection
CV	Connected Vehicles
CVO	Commercial Vehicle Operations
EIC	Editor-In-Chief
IEEE	Institute of Electrical and Electronics Engineers
IOO	Infrastructure Owner Operator
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
JPO	Joint Program Office
MPP	Microsoft Project Document
MPR	Monthly Progress Report
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NEMA	National Electrical Manufacturers Association
NRTM	Needs to Requirements Traceability Matrix
NTCIP	National Transportation Communications for ITS Protocol
OSS	Open Source Software
PMP	Project Management Plan
PRL	Protocol Requirements List
pRS	Proposed Recommended Standard
pUCD	Proposed User Comment Draft
PWS	Performance Work Statement
RI	Reference Implementations
RS	Recommended Standard
RSU	Roadside Unit

RTM	Requirements Traceability Matrix
RTSCF	Roadway Transportation System Cybersecurity Framework
SC	ATC Cybersecurity Steering Committee
SDD	System Design Description
SDR	Standard Development Report
SDO	Standards Development Organization
SE	Systems Engineering
SEMP	Systems Engineering Management Plan
SEP	Systems Engineering Process
SME	Subject Matter Expert
SRS	System Requirements Specification
TBD	To Be Determined
TOCOR	Task Order Contracting Officer's Representative
TRB	Transportation Research Board
UCD	User Comment Draft
USDOT	United States Department of Transportation
V&V	Verification and Validation
WBS	Work Breakdown Structure