COLORADO DEPARTMENT OF TRANSPORTATION **SMART WORK ZONE (SWZ) PLAN**	Project Number:	Project Code:
	Contractor:	
Date:	Traffic Control Contractor:	
Location (MP):	Project Title:	

SWZ Devices

- □ SWZ Data Processing Software
- □ Advance Warning Flashing or Sequencing Arrow Panel (Type)
- □ Automated Flagging Assistance Device
- □ Channelizing Device
- □ Construction Traffic Sign (Panel Size)
- □ Portable Closed Circuit Television
- □ Portable Doppler Radar
- □ Portable Flashing Beacon
- □ Portable Highway Advisory Radio Transmitter
- □ Portable Hybrid Message Board
- □ Portable Microwave Vehicle Radar Detector
- □ Portable Ramp Meter
- □ Portable Traffic Signal
- □ Portable Traffic Speed Monitor
- □ Portable Variable Message Sign Panel
- □ Portable Variable Speed Limit Sign
- □ Portable Weather Monitoring Station

Device Mounting:

- □ Field device trailer
- □ Portable MASH-tested cart
- □ Other:

Use of Existing Infrastructure for Mounting:

I, , approve the use of for the mounting of temporary SWZ devices. The Contractor shall assume all responsibility for the existing asset and will be responsible for maintenance or replacement for the duration of the project.

Asset Owner Signature:	Date:

Inventory of SWZ Devices

Device Locations: Provide a link below for viewing the proposed locations of all SWZ devices within the project limits. Alternatively, attach plan sheets or a schematic at the end of this document.

Device Type		Manufacturer	Make	Model	Quantity	ID/ Serial Numbers
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

SWZ Device Security

Security Requirements: The following minimum requirements must be met for all devices. Describe how these requirements will be met for all devices from page 2.

- Secure devices with a padlock, chain, or other physical security measure.
- Change all default passwords. Meet the minimum password requirements listed in the Materials section, subsection A of the SWZ Devices Specification. It is best practice to change passwords every 60-90 days.
- Utilize devices with field hardened components that prohibit, disable, or restrict unused physical ports, as applicable.
- Use the most recent firmware, operating system, and software patches for all materials. Document all vulnerabilities, so risks are known.

SWZ Data Processing Software Configuration: This project □ will / □ will not be utilizing a SWZ Data Processing Software for remotely monitoring and controlling all devices.

The following minimum requirements must be met for the software. Describe how these requirements will be met during initial software configuration, then complete the supplemental "SWZ Data Access and Alerts" plan.

- Use a centralized authentication source with individual accounts for device access.
  - If centralized authentication is not possible, add general accounts such that dedicated logins can be used for system access and user access accounts can be used for configuration and maintenance.
- Allow for user account creation with specific role-based permissions to fit the authorizations required for the project. Least privileged methodology shall be used when configuring user accounts. Limit the use of built in root or administrative accounts.
- Allow users to reset their username, password, and other profile settings. Multi-factor authentication shall be used for privileged accounts. Provide automatic account lockout after several failed authentication attempts.

Security Checks

Responsible Parties: List all parties responsible for conducting security checks and the CDOT personnel responsible for verifying the security checks were completed and documented for posterity.

Procedure: Define the frequency for conducting security checks during the entire period of construction. Describe the security check procedure and the corrective measures that will occur if one or more devices and/or subsystems fail.

Reporting Requirements: Describe the reporting format, including any digital record printouts from the Data Processing Software. The report must document any failures that occurred during the security check and the corrective measures performed.

Report Submission: Reports will be submitted to CDOT upon completion of the security check via: ☐ Email ☐ In-Person/ Virtual Meeting ☐ Other:	The Contractor will submit the report to no later than days after completion of the security check. will have no more than days to review the report for approval. If the security check does not meet expectations, it must be: ☐ conducted again within days ☐ reviewed and documented by CDOT personnel as an "Acceptable Risk."

Colorado Information Security Policies (CISPs)

List all devices that are not on the QMP, then describe how each requirement will be addressed in the "device verification" column below.

Applicable Devices:

Title	Description	Device Verification
CISP-001: Access Control	ITSP shall specify and document authorized users of the Information System, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.	
CISP-002: Security Awareness and Training	TSP shall, in consultation with the Business Owner, develop and document a security awareness and training program to disseminate the program to all personnel.	
CISP-003: Audit and Accountability	ITSP shall identify events which are relevant to the security of the Information Systems, and the environments in which the systems operate. Auditable events shall include, but not limited to: • Successful and failed logons • Administrative privilege usage • Attempted privilege escalation, privilege escalation, and failed privilege escalation • Change of file or user permissions or privileges • Successful access from known malicious locations • Brute force login attempts, users, and source if identifiable • Intrusion attempts	
CISP-004: Security Assessment and Authorization	ITSP shall develop a Plan of Action and Milestones (POAM) or similar plan for Information Systems to document the organization's planned remediation actions if the systems are found to be lacking in applied security controls.	
CISP-005:Secure Configuration of IT Assets and Software	ITSP shall have and use a formal change control body to review, approve, and track all changes to Information Systems.	
	ITSP shall ensure a configuration management plan is developed, documented, and implemented for the Information System that: • Addresses roles, responsibilities, and configuration management processes and procedures;	

	 - Establishes a process for identifying configuration items (i.e., hardware, software, firmware, and documentation) throughout the system life cycle and for managing the configuration of the system; - Defines the configuration items for the Information System and places the configuration items within the configuration management plan; - Protects the configuration management plan from unauthorized disclosure, dissemination, and modification; and - Describes how to move changes through the change management processes, update configuration settings and baselines, maintain Information System component inventories, control development, test, and operational environments, and develop, release, and update key system documentation.	
	ITSP shall harden systems to include prohibiting, disabling, or restricting the use of unused or unnecessary physical and logical functions, ports, protocols and/or services.	
	ITSP shall scan the network to detect changes to, and review and update, the asset inventory on a regular basis. Automated tools which provide continuous scanning abilities are preferable to a manual scan review; however, if the inventory scan to detect changes is manual, it must be reviewed quarterly.	
CISP-006: Contingency Planning	ITSP and Business Owner shall create a Contingency Plan in which the: - Business Owner identifies essential mission(s) and business functions and associated contingency requirements. - ITSP and Business Owner provide recovery objectives, restoration priorities and metrics. - ITSP and Business Owner address contingency roles, responsibilities, and assigned individuals with contact information. - Business Owner plans for the resumption of essential missions and business functions. - ITSP identifies critical technical and operational assets that support essential missions and functions. - ITSP addresses eventual, full Information System restoration without deterioration of the security safeguards originally planned and implemented. - ITSP and Business Owner ensure the plan is reviewed and approved by key business and Information System leaders or their designees.	
CISP-007: Identification and Authentication	ITSP shall uniquely identify and authenticate agency users and devices (or processes acting on behalf of agency users).v	
	ITSP shall implement multifactor authentication for remote access to the Information Systems for data classified with a Security Category of moderate or high.	
	ITSP shall implement multifactor authentication for local access to system administrative accounts for critical systems.	
	ITSP shall ensure that authenticators have sufficient strength of mechanism for their intended use and include the following: - Minimum password complexity that includes at least nine (9) characters and a mix of upper and lower-case letters, numbers and/or special characters, and - Prohibits password reuse for six (6) generations.	
	ITSP shall store and transmit only encrypted representations of passwords.	

	TSP shall ensure that authentication to a cryptographic module meets the requirements of the Business Owner and that are consistent with all applicable state and federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.	
CISP-008: Incident Response	ITSP shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	
CISP-009: System Maintenance	ITSP shall schedule, perform, document and review records of maintenance and repairs on Information System components in accordance with manufacturer or vendor specifications and/or Business Owner requirements.	
	ITSP shall work with the Business Owner to define acceptable maintenance requirements and windows of allowable system downtime to accomplish such required maintenance.	
	ITSP shall require that the Business Owner explicitly approve the removal of the Information System or system components from organizational facilities for off-site maintenance or repairs.	
CISP-010: Data Protection, Recovery & Sanitization	ITSP shall sanitize digital and nondigital media prior to disposal, release out of organizational control, or release for reuse using required sanitization techniques and procedures in accordance with NIST Special Publication 800-88 Rev.1, Appendix A Minimum Sanitization Recommendations, or applicable federal, state, and Business Owner standards and policies.	
CISP-011: Physical and Environmental Protection	ITSP shall ensure the physical access authorization(s) at entry/exit points to the facility and/or roadside location where the information system resides is enforced by validating the following: • Verifying individual access authorizations before granting access to the facility and/or roadside location; and • Controlling ingress/egress to the facility and/or roadside location using physical access control systems/devices or guards.	
	ITSP shall maintain physical access audit logs for entry and exit points.	
CISP-013: Risk Assessment	ITSP shall conduct an assessment of risk, including the likelihood and magnitude of harm, from an event that could compromise the confidentiality, integrity, and availability of the Information System, with input from Business Owner and prior to placing the Information System into a production state and at intervals throughout the system life cycle according to the data categorization, regulatory requirements, and when new security vulnerabilities are discovered.	
	ITSP shall perform ongoing vulnerability scans on the Information System and applications.	
	ITSP shall employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automated parts of the vulnerability management process by using standards for: • Enumerating platforms, software flaws, and improper configurations; • Formatting checklists and test procedures; and • Measuring vulnerability impact.	
CISP-014: System and Services Acquisition	ITSP and Business Owner shall determine, document, and allocate the resources required to protect the Information System or Information System service as part of its capital planning and investment control process.	
	ITSP shall include, at a minimum, the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the Information System, system	

	component, or Information System service in accordance with the security categorization of the Information System in accordance with Business Owner requirements: • Security functional requirements; • Security assurance requirements; • Security-related documentation requirements; • Requirements for protecting security-related documentation; • Description of the Information System development, test, and production environments; and Acceptance criteria.	
	ITSP shall require the developer of the Information System, system component, or Information System service to: • Perform configuration management during system, component, or service design, development, implementation, and operation; • Document, manage, and control the integrity of changes to configuration Items under Configuration management; • Implement only Business Owner approved changes to the system, component, or service; • Document approved changes to the system, component, or service and the potential security impacts of such changes; and • Track security flaws and flaw resolution within the system, component, or service.	
CISP-015: System and Communications Protection	ITSP shall ensure the Information System protects against or limits the effects of denial of service attacks.	
	ITSP shall ensure the Information System: a) Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b) Implements subnetworks for publicly accessible system components that are physically or logically separated from the internal organizational networks; and c) Connects to external networks or Information Systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the agency's security architecture.	
	ITSP shall ensure the Information System protects the confidentiality and integrity of transmitted information.	
	ITSP shall ensure the Information System terminates the network connection associated with a communications session at the end of the session or after 20 minutes of inactivity according to system functionality and sensitivity needs.	
	ITSP shall establish and manage cryptographic keys for required cryptography employed within the Information System in accordance with applicable state, local, and federal regulatory standards for key generation, distribution, storage, access, and destruction.	
	ITSP shall ensure the Information System implements required cryptographic uses and type of cryptography required for each use in accordance with Information System sensitivity and applicable state and federal laws, executive orders, directives, policies, regulations, standards, and guidance.	
	ITSP shall ensure the Information System requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	
	ITSP shall ensure the Information System fails to a known state preserving security if an Information System failure occurs.	

CISP-016: System and Information Integrity	ITSP shall monitor the Information System to detect: • Attacks and indicators of potential attacks. • Unauthorized local, network, and remote connections.	
	ITSP shall identify unauthorized use of the Information System through active and/or passive system alerts and monitoring of system events/transactions.	
	ITSP shall deploy monitoring devices: strategically within the Information System to collect essential information, and at ad hoc locations within the system to track specific types of transactions in support of incident response.	
	ITSP shall employ automated tools to support near real-time analysis of events.	
	ITSP shall receive Information System security alerts, advisories, and directives on an ongoing basis from external organizations such as the United States Computer Emergency Readiness Team (US-CERT), Multi-State Information Sharing and Analysis Center (MS-ISAC), and the National Institute of Standards and Technology (NIST).	
	ITSP shall alert security incident response personnel when indications of compromise or potential compromise occur.	
	ITSP shall disseminate security alerts, advisories, and directives to personnel responsible for implementing, monitoring, and managing the Information System.	
	ITSP shall employ integrity verification tools to detect unauthorized changes to metadata , software, firmware, middleware, and applications.	
	ITSP shall ensure the Information System performs ongoing integrity checks on software, firmware, and information. The integrity check can occur at a transitional state (e.g., system startup, restart, shutdown, or abort) or security-relevant event (e.g., new threat).	
	ITSP shall ensure the Information System handles and retains information within and output from the Information System in accordance with applicable state and federal laws, executive orders, directives, policies, regulations, standards, and guidance.	
	ITSP shall implement security safeguards to protect memory from unauthorized code execution.	
CISP-017: Security Planning	ITSP shall develop an information security architecture for the Information System that: • Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; • Describes how the information security architecture is integrated into and supports the enterprise architecture; and • Describes any information security assumptions about and dependencies on external services.	
	ITSP shall develop a security plan for each critical or new information system that: a) Is consistent with the organization's enterprise ITS architecture; b) Explicitly defines the authorization boundary for the system; c) Describes the operational context of the information system in terms of missions and business processes; d) Provides the security categorization of the information system including supporting rationale; e) Describes the operational environment for the information system and relationships with, or connections to, other information systems;	

	f) Provides an overview of the security requirements for the system; g) Identifies any relevant overlays, if applicable; and h) Describes the security controls in place or planned for meeting those requirements including a rationale for custom configuration decisions.	
CISP-018: Acceptable Use Policy (AUP)	Entire document.	
CISP-019: Continuous IT Vulnerability Management & Patching	Entire document.	

SWZ Device Maintenance

SWZ Vendor Name:	Vendor Contact Information:

Additional Relevant Contacts:

Contact Information:

Device Power: □ Solar □ Battery □ Gas □ Other:	**Device Communications:** □ None □ Cellular modem □ Satellite □ Radio □ Other:

Use of Local or Regional Power:
I, , approve the use of for SWZ devices. I will track all utility information per Procedural Direction 90.1 "Utility Account Management" and take ownership of all coordination with CDOT ITS, as needed.

Engineer Signature:	Date:

Device Maintenance Procedures: Describe the process for maintaining continuous operations for each SWZ device.

SWZ Device Operational Test

Operational Test Procedure: Describe the traffic control required for the operational testing period and the procedures for ensuring all devices are operating in a fully functional manner. Provide an explanation if support from the SWZ Vendor or other parties is required.

WZDx Device Feed: This operational test procedure □ will / □ will not involve pushing a sample WZDx-compliant device data feed to CDOT. The sample data feed will include the following devices and types of data:

SWZ Device Payment

Method of Measurement: All SWZ devices will be paid on a □ daily / □ monthly basis. The following devices will be paid for each unit that is deployed:

- □ Channelizing Device (SWZ)
- □ Construction Traffic Sign (Panel Size) (SWZ)
- □ Portable Flashing Beacon (SWZ)

The prorated daily unit cost will be utilized for pay deductions of non-operational devices. For projects using the daily method of measurement, this is simply the daily cost of the device.

Device Type		Prorated Daily Unit Cost	Quantity	Total Daily Cost
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

SWZ Messaging Plan

****This is a supplemental plan that should only be submitted if a messaging device is deployed. ****

Messaging Devices: The following messaging devices will be deployed on the project:

- □ Construction Traffic Sign (Panel Size) (SWZ)
- □ Portable Hybrid Message Board (SWZ)
- □ Portable Variable Message Sign Panel (SWZ)

Sign Legends: List the size and legend for each deployed sign.

Sign Message: List all potential messages that can be displayed for each sign and the proposed frequency of updates. Identify the use case for each message. Include the default message that will be displayed in cases where there is insufficient data.

Messaging Conflicts: To prevent conflicts in messaging between SWZ devices and permanent message boards, the Engineer must coordinate with RTO daily. Daily coordination between the Engineer and RTO will occur via:

- □ Email Report
- □ Virtual Meeting
- □ In-Person Meeting
- □ Other:

SWZ Data Access and Alerts

****This is a supplemental plan that should only be submitted if a data processing software is used. ****

SWZ Data Processing Software Setup:

Name and Contact Information (Phone/ Email)		**Relation to Project** (Contractor/ Engineer/ CDOT)	**Level of Access**
			□ Read-Only □ Editor □ Admin □ Other:
			□ Read-Only □ Editor □ Admin □ Other:
			□ Read-Only □ Editor □ Admin □ Other:
			□ Read-Only □ Editor □ Admin □ Other:
			□ Read-Only □ Editor □ Admin □ Other:
			□ Read-Only □ Editor □ Admin □ Other:
			□ Read-Only □ Editor □ Admin □ Other:

Work Zone Data Exchange Requirements	
API Key and Authentication Token: This must be obtained from CDOT ODM.	Planned Event Identifier Number: This must be obtained during the planning process.
Notes: All coordination with CDOT ODM should occur through the Engineer.	

Device Alerting	
All Alert Types (with associated devices):	
Alert Recipients	**Method of Delivery**
	□ Text Message □ Email □ Both
	□ Text Message □ Email □ Both
	□ Text Message □ Email □ Both
	□ Text Message □ Email □ Both
	□ Text Message □ Email □ Both
	□ Text Message □ Email □ Both
	□ Text Message □ Email □ Both
	□ Text Message □ Email □ Both

SWZ System Plan

**This is a supplemental plan that should only be submitted if a SWZ System is used. **

SWZ Subsystems: The following subsystems will be deployed on the project:

- □ Queue Warning
- □ Dynamic Lane Merge
- □ Travel Time Information
- □ Incident Detection (Project Surveillance)
- □ Speed and Volume Monitoring
- □ Construction Vehicle Egress Notification
- □ Overheight Vehicle Detection
- □ Hazardous Condition Notification
- □ Temporary Ramp Metering
- □ Variable Speed Limit

Subsystem Configuration:

System Training:

Subsystem and Device Communication:

SWZ System Operational Test

Operational Test Procedure: Describe the traffic control required for the operational testing period and the procedures for ensuring all subsystems are operating in a fully functional manner. Provide an explanation if support from the SWZ Vendor or other parties is required.

SWZ Reliability and Accuracy Requirements
Test Procedures: Describe the procedures for meeting all reliability and accuracy requirements of the SWZ System. Include the schedule for field inspections and processes for resolving any system malfunctions or data concerns. Provide an explanation if support from the SWZ Vendor or other parties is required. Describe how the results will be documented and submitted to the Engineer.

SWZ System Logic

Background: Explain the historical data or real-time observations that will be used to define the logic thresholds for all relevant SWZ subsystems. Identify which sensors will be utilized for messaging automation in a subsystem.

Devices and Input Logic	**Result** (Free Flow- above 45mph)	**Result** (Moderate- between 20 and 45mph)	**Result** (Heavy- below 20mph)

Devices and Input Logic	**Result** (Free Flow- above 45mph)	**Result** (Moderate- between 20 and 45mph)	**Result** (Heavy- below 20mph)

Contractor SWZ Plan Verification

I, , affirm that all information submitted in this plan is accurate and complete, given current understanding of construction phasing and operations. This plan is being submitted at least 30 days prior to SWZ device setup. I will provide written confirmation to the Engineer seven days in advance of any proposed changes to this plan.

This plan contains these sections:

- ☐ SWZ Device Plan (Pages 1-11)
- ☐ SWZ Messaging Plan (Page 12)
- ☐ SWZ Data Access and Alerts (Pages 13-14)
- ☐ SWZ System Plan (Pages 15-18)

Contractor Signature:	Date:

CDOT Engineer Acceptance

I, , approve this SWZ Plan in its entirety with no proposed revisions. I will verify that the plan is upheld with no deviations for the duration of the project. I will forward this plan to the CDOT TS&E Representative and to CDOT ITS at cdot_its_support@state.co.us for review.

I, , do not approve this SWZ Plan and propose the following revisions:

Revisions should be made in a timely manner and the SWZ Plan should be resubmitted for final approval. I will forward this plan to the CDOT TS&E Representative and to CDOT ITS at cdot_its_support@state.co.us for review.

Engineer Signature:	Date:

CDOT Traffic Safety & Engineering Services Acceptance

I, , approve this SWZ Plan in its entirety with no proposed revisions.

I, , do not approve this SWZ Plan and propose the following revisions:

Revisions should be made in a timely manner and the SWZ Plan should be resubmitted for final approval.

Representative Signature:	Date:

CDOT ITS Acceptance

I, , approve this SWZ Plan in its entirety with no proposed revisions.

I, , do not approve this SWZ Plan and propose the following revisions:

Revisions should be made in a timely manner and the SWZ Plan should be resubmitted for final approval.

Representative Signature:	Date: